IMPLEMENTACIÓN DE UNA HERRAMIENTA OPEN SOURCE COMO SISTEMA DE SEGURIDAD REACTIVA EN ESCENARIOS EMPRESARIALES PYMES, COMO SOLUCIÓN DE SEGURIDAD A BAJO COSTO

Carlos Iván Téllez Gutiérrez[·]

RESUMEN

El objetivo de este documento es poder aportar una herramienta Open Source y conocimientos teóricos necesarios en la implementación de una solución de seguridad informática, y poder animar a la PYMEs que es viable poder adquirir software sin tantos costos de hardware especializado para poder cumplir con niveles de seguridad requeridas más comunes, como lo es un firewall, portal cautivo, Antivirus y filtrado WEB.

Este Open Source, puede llegar a ser un Software de Seguridad Reactivo (**SSR**) de bajo costo que ayuda a tener contramedidas contra los diferentes tipos de ataques y amenazas en seguridad informática, a los que se ven comprometidas las comunicaciones e información de las PYMES.

Las amenazas y los diferentes ataques cibernéticos se deben a la baja o nula protección de las Pymes como lo pueden ser puertos abiertos, malware, ausencia de controles de seguridad en los enlaces de internet por demanda (comúnmente instalados como ADSL)

Sin protección de una DMZ y un firewall, falta de control de WEB que permita anular esos ataques.

El poder implementar un Software SSR basado en Open Source, puede ayudar a una PYME con configuraciones básicas y hardware sencillo a llegar a protegerse a un muy buen nivel de gestión.

· Universidad Veracruzana,catellez@uv.mx, Xalapa, Veracruz

Palabras clave

ADSL, LAN, ISP, Antivirus, Firewall, PYME (Pequeña y Mediana Empresa), amenazas tecnológicas, seguridad informática, Software de Seguridad Reactivo (SSR)

INTRODUCCIÓN

La rapidez con la que están absorbiendo tecnología las PYMES y que la están adaptando a su modelo de negocio para eficientar y automatizar procesos para diferenciarse de su competencia en servicio y prontitud de respuesta, organización y mejorar las transacciones comerciales y la integridad de la información de los clientes.

Las PYMES gracias a que los costos de tecnología y de acceso a Internet han ido en decremento con el paso del tiempo y los diferentes servicios hacia los clientes y procesos internos y externos como correo electrónico, pago de impuestos, servicios en la nube Internet, extranet, entre otros, se observa que se ha incrementado también el nivel de riesgos y ataques derivados de las vulnerabilidades y conocimientos técnicos que en esta época la brecha digital en las PYMES crezca debido a la implementación de nuevas tecnologías.

La gran diversidad de acceso a Internet de los ISP (Internet Service Provider, Proveedores de servicio de Internet), deja a la deriva a las PYMES con poca o nula protección en el acceso a una red local (LAN, Local Area Network) y hacia contenidos en Internet no alineados a los procesos de negocio en donde lleva que este sea el punto ideal para accesos no autorizados, ataques del tipo Denial of Service (DoS) y virus informáticos.

Cualquier persona con conocimientos básicos de redes y protocolos de comunicación aunada a las herramientas y tutoriales disponibles en Internet de algún estudio o tutorial de vulnerabilidades de alguna marca comercial o abierta de sistema operativo de red, marcas de Routers dinámicos (ADSL), Switches, entre otros pueda accesar a una red de cómputo.

Por otro lado, para los Hackers, aumenta más la atención que las PYMES sean débiles en cuanto a su protección perimetral, Interna y sobre todo a su acceso de la red desde Internet.

La realidad de la PYME en el entorno de TI

Aunque mucho de las herramientas que se tienen hoy para poder tener contramedidas hacia un ataque, vulnerabilidad o un virus informático, los usuarios de las PYMES no poseen una cultura informática de habilidades, capacidades técnicas y el conocimiento de las amenazas a la seguridad y de las técnicas apropiadas de control a fin de proteger su infraestructura de red y comunicación (Edgar Tello Leal, 2008) han evolucionado muy rápido y paralelamente al desarrollo tecnológico, va también en aumento una gran complejidad de los ataques(HPE Security Research Cyber Risk Report, 2016) debido a la curva de aprendizaje de alguna vulnerabilidad o sobre todo de algún debilidad encontrada en el software o red.

Por lo anterior, Las empresas, especialmente las PYMES, deben mantenerse a la vanguardia sobre el correcto uso de las tecnologías, de cómo mantener a salvo al menos su presencia dentro de la red de Internet para garantizar su integridad digital.

El cómo protegerse es un tema el cual existe un gran abanico de posibilidades en hardware y software pero que al momento de ver la realidad económica en cuestión de los costos, es un problema. La otra cuestión, es de poder asesorarse con algún experto en la materia que pueda prestar la debida atención a lo que la PYME necesita como requerimiento mínimo en protección en amenazas de ataques, contramedidas de espionaje informático, accesos no autorizados, etc.

La importancia de las PYMES en salvaguardar su información.

Las Pymes se encuentran en la obligación tecnológica de proteger su volumen de información todas sus bases de datos de conocimiento de una manera ágil, generando a sus clientes la suficiente confianza y credibilidad para poder realizar sus transacciones comerciales de forma segura, rápida y eficiente.

Vulnerabilidades que se exponen las PYMEs hoy en día.

Toda organización maneja información crítica debe estar consciente que para poder hablar seguridad informática, se pueda identificar primero a los diferentes tipos de ataques y amenazas a los que se ven expuestas como:

- **Phising**: Es la suplantación de identidad y que se comete mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta. Por ejemplo, la suplantación de un banco que solicita actualizar el pasword de acceso a una cuenta bancaria.

- **DDOS**(Distributed Denial of Service): Se traduce como ataque distribuido y denegación de servicio, consiste en atacar al servidor desde otras computadoras para que deje de funcionar.

- **Malware**: es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario

- **Spyware**: El spyware es un software que recopila información en una computadora y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del mismo.

- **Bugs**: Vulnerabilidades de un proveedor o falla mal intencionada por un problema técnico en algún Software

- **Spam:** . Correo basura o mensajes no solicitados, no deseados o de remitente desconocido.

- **Botnet**. Ataques que puede controlar todos las computadoras infectadas de forma remota

- **Fuga de Información**: Mediante medios electrónicos se roba información sensible de la empresa por parte de empleados o terceros usando métodos de transferencia electrónica.

- Intrusión remota. Ingreso externo no autorizado a un equipo de cómputo usando la infraestructura de conectividad de la empresa.

- **Fuerza Bruta**: Se emplea software automatizado para generar una lista larga de posibles contraseñas de acceso, para ingresarlas en la cuenta de un usuario .

- **LDAP** (Lightweight Directory Access Protocol): Es un Protocolo Ligero/Simplificado de Acceso a Directorios el cual que hace referencia a un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red

- **Inyección de SQL**. es una técnica donde un atacante crea o altera comandos SQL existentes para exponer datos ocultos, sobrescribir los valiosos, o peor aún, ejecutar comandos peligrosos a nivel de sistema en el equipo que hospeda la base de datos.

Internet, los riesgos en las PYMES

El incremento exponencial del crecimiento de Internet, ha permitido que las PYMES sean más competitivas y más eficaces en sus procesos que ahora se encuentran interconectados y que ayuda mucho a eficientar los procesos internos y publicar servicios a los clientes externos en Internet.

Como consecuencia de esto se han visto expuestas a una serie de riesgos y amenazas inherentes a la implementación de transacciones comerciales a nivel nacional e internacional. Este problema impacta de manera negativa a las PYMES ya que para tener los mínimos requerimientos de seguridad de la información,

se deben establecer y mantener acciones que cumplan con tres requerimientos (Borghello, 2001).

- **Confidencialidad**: Previene el acceso no autorizado ya sea en forma intencional o no intencional a la información. La pérdida de la confidencialidad puede ocurrir de muchas maneras, como por ejemplo con la publicación intencional de información confidencial de la organización.
- **Integridad**: Que no se realicen modificaciones no autorizadas por personal autorizado a los datos o procesos y sean consistentes tanto interna como externamente.
- **Disponibilidad:** Tiene que ver con asegurar un acceso confiable y oportuno a los datos o recursos para el personal apropiado.

Por qué implementar un SSR en una PYME

La seguridad hoy en día es un tema importante en las TI dentro del contexto de las PYMES, pero la mayoría no tiene tan claro que la seguridad ya debe ser parte la cultura organizacional. Dentro de los conceptos de la organización de empresa y asignación de presupuesto, debería asignarse como prioridad el dedicar recursos a la seguridad, pero en muchas es hasta nula, hasta que se presenta un evento o en el peor de los casos un desastre.

Ante los riesgos informáticos actuales, las PYMES necesitan empezar a tomar precauciones con el fin de impedir ataques o infecciones externas

Por otro lado, el proteger a la LAN desde fuera de la red de la empresa, ayuda a evitar accesos no autorizados, con el objetivo de minimizar vulnerabilidades en los sistemas de la LAN.

Las grandes Empresas tienen el poder económico y técnico para poder implementar seguridad (Deloitte, 2007) y enfrentarse a una crisis de seguridad de información ya sea Interno o externo a la Red.

El poder proteger la LAN de una PYME y proveer seguridad de la información ya no es una opción más de inventario de la empresa, si no que surge ahora la necesidad de una estrategia de seguridad, bajo costo y una implementación alineada con los controles que se definan e instaurar una política clara al respecto.

Ni las empresas grandes se salvan de implementar seguridad, ya que en los últimos años, se han visto diferentes ataques a empresas como PlayStation de Sony, PayPal, Paginas gubernamentales, entre otros incidentes que se han reflejado en el robo de identidad de los usuarios, robo de información financiera(cuentas, claves bancarias, claves de seguridad de tarjetas de crédito), robo por mensajes de correo del tipo Phising, y que para los clientes y usuarios han dejado una mala imagen de estas empresas y accionistas, cuestionando el manejo de seguridad que se le está brindando a los datos.

Una de las soluciones que se han desarrollado para contrarrestar las amenazas tecnológicas han sido los Firewalls, Anti-spam, AntiMalware, Antivirus, etc pero el crecimiento de amenazas y los diferentes tipos de ataque, hacen que estas soluciones sean caros adquirirlas una por una y que sea poco accesibles en el presupuesto para las PYMEs.

Para el caso de una LAN de una PYME, el poder instalar una herramienta que pueda cubrir los aspectos de Confidencialidad, Integridad y Disponibilidad a un bajo costo,

Protegiendo a la seguridad física y lógica de una PYME un SSR.

Una de las preguntas que se debe de hacer una PYME es: ¿qué se debe proteger?.

Es claro mencionar que en cuestión de continuidad de negocio, los elementos a proteger sean primeramente los DATOS.

En segundo lugar, el hardware en donde estos residen, se modifican, resguardan y se accesan, es decir; el conjunto de componentes que integran la parte física de la red LAN y el hardware de cómputo.

Como tercer elemento, la parte LÓGICA, que es el conjunto de aplicaciones, sistemas operativos y programas de red que ayudan a los procesos de negocio de las PYMES.

Para poder proteger a una PYME brindándole una herramienta de seguridad que cumpla con los requisitos de bajo costo, fácil instalación, requerimientos de hardware de costo accesible y velocidad y de cobertura (NETGEAR, 2011)

con una herramienta de seguridad se necesita un que cumpla con ciertos requisitos de:

- Filtrado de origen a destino de IP, protocolo IP, puerto de origen y destinación para TCP y UDP tráfico
- Balanceador de carga por terminales para conexiones simultaneas con reglas de base
- Politicas de enrutamiento con alta flexibilidad para la seleccion del gateway sobre las reglas de base para el equilibrio de banda, failover, WAN multiple, backup sobre mas ADSL, etc…
- Filtracion transparente en capa 2.
- Posibilidad de inhabilitar la **filtración** (firewalling) o la opción de solo **router**

En el ambiente de herramientas OPEN SOURCE, pfSense cumple mucho de estas características y tiene una gran ventaja para una PYME, es una distribución gratuita. Basada en FreeBSD, tiene el potencial de ser un Firewall y Router a la vez, sustituyendo las cajas de enlaces que los ISP instalan. Incluye una gran lista de paquetes que permiten expandir fácilmente las funcionalidades sin comprometer la seguridad del sistema.

Pfsense(https://pfsense.org/), cuenta con un gran respaldo de descargas e instalaciones por todo el mundo ya que cuenta con más de 1.000.000 descargas y innumerables instalaciones en todo el mundo y puede ser instalado en una gran variedad de equipos.

Dentro de sus características cuenta con firewall que sirve como un área de la LAN que audita todo el tráfico de Internet entrante y saliente y que permite circular, permitiendo controlar el tráfico y que bien configurado y administrado evita en gran medida que los hackers lo superen y por supuesto ayuda a mantener a salvo los datos confidenciales de las PYMEs y permite la monitorización y registro de las bitácoras de los servicios utilizados internos y externos al usar Internet y demás protocolos requeridos.

Pfsense por ser una distribución basada en BSD, se adaptan muy bien a los niveles de seguridad actuales ofrece ventajas de seguridad informática que las PYMES pueden adquirir.

Caso de éxito de PYME BUSINESS CENTERS Xalapa.

BUSINESS CENTERS Xalapa, es una PYME que ofrece servicios de oficina virtual y oficinas físicas localizadas en la ciudad de Xalapa. Dentro de los usuarios que requieren velocidad, seguridad y disponibilidad de los servicios se encuentran: Nestlé, Profuturo, Asistek, entro otros.

Se utilizó una computadora Intel Celeron Core 2 Duo 1.8 Ghz, 4 GB Ram, HDD 250 GB y 2 tarjetas de red Realtek. Enlace de Internet Telmex FTTH 20 Mbps, Switch LAN Linksys de 16 puertos y AP Linksys.

Módulos Instalados:

-Portal Cautivo y Radius

-Antivirus, proxy y filtrado de contenido.

-Módulo HAVP, que es un módulo integrado de proxy y antivirus para el contenido Web

-Squid y Ligtsquid para generación de estadísticas para analizar reportes de consumo de ancho de banda, páginas visitadas y número de ingresos, entre otros, con el fin de tomar decisiones y para procesos de auditoría.

- Firewall, con reglas para que garanticen la mayor protección posible sin afectar el rendimiento, por ejemplo: permitir que los usuarios que vengan de una WAN accedan a una Intranet mediante protocolo https por el puerto 443.

- VPN, para acceso remoto a oficinas

- Squidguard, que ayuda a las usuarios de las PYMES de modo seguro, que los contenidos de navegación en internet, se haga correcto uso de los recursos alineados al modelo de negocio de los procesos de la empresa.

CONCLUSIONES

Uno de los retos de las Pymes es poder adaptarse a los requerimientos de seguridad informática para evitar las diferentes amenazas y las diferentes protecciones que se pueden hacer en las aplicaciones de red de servicio como correo, transacciones electrónicas, contenido válido de tráfico de Internet, entre otros.

El tema del poder adquirir una herramienta SSR y que Pfsense permite a las Pymes dentro de sus inversiones, considerar que no tiene costo y que su mantenimiento es bajo sobre la maquinaria que se instale

Pfsense sirve para el concepto que llamamos SSR, como una herramienta de aseguramiento de LAN y acceso a Internet, siendo una plataforma que le ayuda a una PYME a tener un punto de equilibrio económico y operativo.

Trabajos a futuro

Describir y Analizar una herramienta que PfSense acaba de liberar y es el **p0f**, la cual es una avanzada herramienta de red para huellas dactilares digitales que habilita la **filtración** a travez el sistema operativo al inicio de la conexión. Permitiendo saber realmente quién es el usuario que esta atrás del dispositivo.

REFERENCIAS

- (Edgar Tello Leal, 2008), “Las tecnologías de la información y comunicaciones (TIC) y la brecha digital: su impacto en la sociedad de México”, http://www.uoc.edu/rusc/4/2/dt/esp/tello.pdf)
- (HPE, Security Research Cyber Risk Report 2016), https://ssl.www8.hp.com/mx/es/ssl/leadgen/secure_document.html?objid=4AA6-3786ENW&siebelid=560016101&sectionid=pdf&returnurl=%2Fmx%2Fes%2Fsecure%2Fpdf%2F4aa6-3786enw.pdf&simpletitle=cyber%20risk%20report&subbu=tsg.software&parentPageName=3.0&analytics_page_name=3.0&parentUrl=http%3A%2F%2Fwww8.hp.com%2Fmx%2Fes%2Fsoftware-solutions%2Fcyber-risk-report-security-vulnerability%2F&compURI=tcm%3A230-1906136&fv=FLEX2%20SW3&metrics_asset_value=eb&bu=tsg&st=%2Fmx%2Fes%2Fsoftware-solutions%2Fcyber-risk-report-security-vulnerability&as=software&wsi=r11374&cu=false)
- (Borghello, 2001) “Seguridad Informática: sus implicaciones e implementación”. Tesis de Licenciatura en Sistemas, Universidad Tecnológica Nacional, Argentina, 2001
- (Deloitte, 2007), I. Brightman, J. Buith. “Treading Water. The 2007 Technology, Media & Telecommunications Security Survey”, Deloitte, 2007.)
- (NETGEAR, 2011) “Dispositivo ProSecure Para la gestión Unificada de las amenazas”. Online [Mar. 2011]. [11]G