Dispositivos de bajo costo como hardware para implementar herramientas de apoyo a la seguridad informática

Low-cost devices such as hardware to implement support tools for computer security

Alexander Larrahondo Núñez

Edgar Mauricio López Rojas

Universidad Nacional Abierta y a Distancia, Colombia

Resumen

La masificación de los servicios de telecomunicaciones, el acceso a Internet, los bajos precios de la electrónica de consumo, la telefonía móvil y el Internet de las cosas entre otros, han generado un panorama complejo desde el punto de vista de los riesgos de ciberseguridad, lo que lleva a que las grandes empresas y los gobiernos pueden invertir una gran cantidad de recursos para la compra y operación de plataformas de seguridad que les ayuden a minimizar estos riegos, pero para las pequeñas y medianas empresas (pymes) este tipo de inversiones no son posibles, lo que las convierte en un blanco ideal de los ciberdelincuentes. La posibilidad de utilizar dispositivos de bajo costo como hardware sobre el que se puedan implementar herramientas de apoyo a la seguridad informática abre un nuevo espectro de posibilidades que puede cubrir también necesidades en el hogar moderno, donde también hay varios dispositivos conectados a Internet que pueden ser víctimas de ataques.

Palabras clave: Raspberry pi, ciberseguridad, IDS.

Abstract

The massification of telecommunications services, Internet access, the low prices of consumer electronics, mobile telephony and the Internet of Things, among others, have generated a complex panorama from the point of view of Cybersecurity risks, large companies and governments can invest a large amount of resources for the purchase and operation of security platforms that help them minimize these risks, but for small and medium-sized enterprises (SMEs) this type of investment is not possible, which it becomes an ideal target for cybercriminals. The possibility of using low-cost devices as hardware on which IT security support tools can be implemented opens up a new spectrum

of possibilities that can also cover needs in the modern home, where there are also various devices connected to the Internet that can be victims of attacks.

Keywords: Raspberry pi, ciberseguridad, IDS.

1. Introducción

Con el impulso que se dio a la digitalización de la información a raíz de la pandemia de Covid-19, las compañías que no tenían presencia en Internet o que esta no se había consolidado, debieron realizar esfuerzos técnicos y económicos para digitalizar sus negocios con el fin de poder comercializar productos y servicios de manera digital ante la imposibilidad de hacerlo de manera presencial, como resultado de las restricciones de movilidad impuestas por muchos de los gobiernos como estrategias para evitar y controlar los contagios de Covid, y con ello llegaron también los riesgos asociados a la ciberseguridad.

Según Bancoldex –Banco de Desarrollo Empresarial– las pequeñas y medianas empresas (pymes) hace referencia al grupo de empresas pequeñas y medianas con activos totales superiores a 500 salarios mínimos mensuales legales vigentes (SMMLV) y hasta 30.000 salarios mínimos legales vigentes, clasificación que está reglamentada en la ley 590 del 2000 y sus modificaciones; la ley es conocida como Ley Mipymes. Según esta misma ley las pymes se clasifican así:

- Microempresa: personal no superior a 10 trabajadores, activos totales inferiores a 501 SMMLV

- Pequeña empresa: personal entre 11 y 50 trabajadores, activos totales mayores a 501 y menores a 5.001 SMMLV

- Mediana empresa: personal entre 51 y 200 trabajadores, activos totales entre 5.001 y 15.000 SMMLV

Las redes del hogar y de las pymes han madurado durante los últimos años e incluido nuevos y variados dispositivos que aumentan la cantidad de dispositivos tradicionales en este tipo de redes y que agregan nuevas y muchas veces no descubiertas vulnerabilidades a la misma. El panorama ya era complejo con computadores de escritorio, portátiles, tablets y teléfonos, si a ese ambiente ya heterogéneo sumamos IoT, en donde podemos conectar bombillos, enchufes, parlantes, neveras y demás, ya los grandes fabricantes de sistemas operativos para pc y celulares como Microsoft, Linux, IOS, Android

no daban abasto atendiendo con toda su experiencia las vulnerabilidades de sus plataformas, cada una con sus particularidades de implementación, ahora los fabricantes de tostadoras, cámaras de videovigilancia, fabricantes de bombillos y demás, intentando afrontar procesos de SDLC sin madurar, en el mejor de los casos, para proveer a sus clientes con una experiencia de conectividad a Internet medianamente segura. La contracción del mercado de la electrónica y aquellas industrias que hacen uso intensivo de la misma a raíz de la escasez de chips ocasionada por la pandemia de Covid mermó el crecimiento del número de dispositivos de IoT, pero aun así para el año 2022 ya se tenían 12.2 billones de dispositivos conectados y sus principales y conocidas debilidades como son el mal uso de autenticación, controles de acceso inadecuados y vulnerabilidades de desbordamiento de enteros sumados a malas prácticas como el uso de contraseñas por defecto, ya generaban que estos dispositivos fueran utilizados para generar ataques de denegación de servicio a terceros, fugas de información y varios tipos de ataques adicionales.

El amplio portafolio de fabricantes para soluciones de seguridad presentan también ofertas diferenciadas para pymes, las soluciones de seguridad tienden a integrar el hardware y el software con el fin de optimizar su funcionamiento, el resultado de esas integraciones son generalmente diferentes modelos de appliances que para las pymes serían los modelos de entrada con prestaciones o capacidades técnicas moderadas, y, que sin embargo, siguen representando una inversión mayor dentro del presupuesto de pequeñas organizaciones que difícilmente puedan tener consolidadas áreas de tecnología y menos aún áreas de seguridad, dificultando con ello una asertiva evaluación y comparación de soluciones y/o productos de seguridad que puedan adquirir, poniendo en riesgo sus capacidades de inversión en tecnologías de seguridad que ayuden a la organización a atender sus riesgos más relevantes

El acceso entonces a soluciones de seguridad open source que además se puedan ejecutar en SBC de bajo costo (Single Board Computer) abre un amplio panorama desde el punto de vista de la relación costo/beneficio para que las pymes puedan acceder a soluciones de seguridad informática que les permitan implementar y/o mejorar su postura de seguridad.

2. Contexto Colombia

Según la XXII Encuesta Nacional de Seguridad Informática realizada porla Asociación Colombiana de Ingenieros de Sistemas – ACIS– del año 2022, los tipos de incidentes de seguridad que más se presentan son errores humanos con el 38 %, phishing 32 %, acciones de ingeniería social 25 %, accesos no autorizados a la web 17 %, fraude electrónico 15 %, virus/caballo de Troya 15 %, ataque de aplicaciones web (XSS, Sql Inyection, etc.) 15 %, ransomware 12 % y ciberataques (APT) 12 %, de esta estadística podemos inferir que seguir trabajando en la cultura de seguridad puede ayudar a disminuir varios de los incidentes que se presentan usualmente en las organizaciones, pero también que para varios de los demás incidentes el uso de herramientas de seguridad informática como IDS/IPS pueden ser de mucha ayuda para automatizar tanto la detección como la respuesta a estos eventos, precisamente fortaleciendo los controles de seguridad en donde las debilidades de cultura de seguridad genera riesgos significativos para las organizaciones.

De esta misma encuesta de ACIS revisando los datos de a quien se notifican los incidentes de seguridad la encuesta muestra que la notificación se hace a los directivos de la propia organización con el 61 %, al equipo de atención de incidentes (CSIRT) 47 %, a las autoridades nacionales (Policía, entidades regulatorias, Fiscalía, etc.) 33 %, al asesor legal 23 %, autoridades locales/regionales con el 15 % y que no se denuncia con el 5 %, para esta información se puede inferir que si bien en la mayoría de los incidentes los directivos de la organización son notificados, se debe seguir trabajando desde los aspectos regulatorios con el fin de que el reporte de este tipo de eventos sea obligatorio para todas las entidades, con el fin de tener un panorama más claro de los incidentes, sus tipologías, las acciones a tomar para su contención y remediación y aún más importante para la definición de políticas públicas de protección.

En un contexto donde en Colombia no se tiene una agencia nacional de ciberseguridad que era una propuesta que estaba evaluando el Gobierno, que debería tener como una de sus principales funciones la articulación de las capacidades de ciberseguridad y ciberdefensa del estado para la protección de sus ciudadanos en relación con la ciberseguridad y ciberdefensa, capacidades que se definieron en el documento Conpes 3701 "Lineamientos de política para ciberseguridad y ciberdefensa" documento del año 2011, que lamentablemente no se ha visto implementado de manera técnica y articulada a pesar de los múltiples incidentes de seguridad que han sucedido recientemente, y, que, apoyado con la declaración de obligación del Estado de diseñar una ruta de atención de vulnerabilidades y respuesta a incidentes que

quedo también definida en el documento Conpes 3995 "Política nacional de confianza y seguridad digital" de 2020 y que tampoco está definida.

En teoría, en Colombia tenemos los lineamentos necesarios para definir, operar e instrumentalizar un ecosistema que ayude a fortalecer las capacidades del estado para proteger a sus ciudadanos, pero en la realidad todas estas iniciativas se han quedado en el papel y en la práctica los incidentes de seguridad que se han sucedido y los que con seguridad se van a suceder se tendrán que seguir atendiendo desde las capacidades de las organizaciones sin ninguna articulación eficiente de parte del Estado que no demuestra voluntad para definir de manera asertiva e integral acciones eficaces de defensa en el ciberespacio.

El sector de la pymes no es ajeno a estas circunstancias y al tener menores capacidades técnicas, presupuestales y aún menos apoyo del Gobierno para asumir los restos de ciberseguridad es víctima fácil de los ciberdelincuentes, los ataques no discriminan el tamaño de la organización, según estadísticas del DANE para el año 2022, en Colombia son más de 5.15 millones de pymes que generaron $56.6 billones de pesos en valor agregado al país, sin embargo, de esa misma información evidencia también que 1.94 millones de micronegocios se crearon porque no se tenían otras alternativas de ingresos lo que no genera además confianza de que la seguridad de la información sea una prioridad para estas pymes.

3. Costos de las brechas de datos a nivel mundial

Según la encuesta de IBM: Reporte de brechas de datos 2022, que se realiza a nivel mundial y que incluye grandes compañías no pymes, pero que nos da un entendimiento de que los ciberataques acarrean costos financieros elevados, para el año 2022 el costo promedio a nivel mundial de una brecha de datos es de USD $4.35 millones de dólares con un incremento del 2.6 % con respecto al año anterior y un 12.7 % de incremento contra el valor reportado en el 2020, el dato para Latinoamérica en el año 2022 USD $2.80 millones de dólares mientras que para los EUA es de USD $9.44 Millones de dólares, así mismo el tiempo promedio de la identificación y contención de una brecha de datos de 277 días.

Estas estadísticas muestran el impacto económico que puede generar una brecha de datos y dimensiona el impacto que puede tener en el factor económico en una organización, si estos valores se extrapolan a las pymes, la menor brecha de datos sacará del mercado a cualquier pyme

4. Conceptos teóricos

Los dispositivos de bajo costo conocidos en inglés como "SBC Single Board Computer" en términos simples son computadores de un tamaño similar al de una tarjeta de crédito que ofrecen capacidades de cómputo que, si bien no son excepcionales, si ofrecen por un valor económico menor al de equipos dedicados y/o computadores personales o portátiles comunes, capacidades de cómputo que pueden ser suficientes para poder instalar, compilar y/o ejecutar sobre ellas de manera adecuada una amplia variedad de herramientas de seguridad informática.

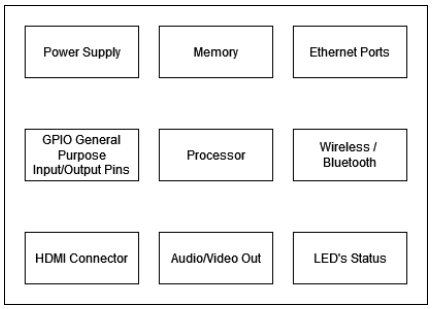

Figura 1. Diagrama de bloque de un SBC. Fuente: propia.

Los SBC tal como observamos en la Figura 1, cuentan al menos con fuente de poder, memoria, procesador, interfaces de entrada y salida de video y audio, puertos Ethernet, conexión Wireless y/o bluetooth, entrada salida de propósito general (GPIO), que permiten configuraciones tanto generales como específicas dependiendo de las funcionalidades como leer/escribir datos binarios para activar determinadas funciones que soporte el SBC generalmente para conectar dispositivos electrónicos como transistores, sensores, motores de paso, y otros, allí se pueden conectar también placas específicamente diseñadas para ampliar las funcionalidades de los SBC.

Estas capacidades de cómputo correctamente aprovechadas en conjunto con algunas versiones de soluciones de seguridad informática de software libre son suficientes para configurar una amplia gama de herramientas de seguridad que pueden ayudar a que las pymes fortalezcan su postura de seguridad.

Uno de los SBC más conocidos es la Raspberry PI lanzada en el año 2012 por la Raspberry Pi Foundation, organización benéfica ubicada en el Reino Unido con el objetivo de facilitar el acceso a la educación informática al proveer este tipo de placas de bajo costo con propósitos educativos, el dispositivo original tenía un procesador de un solo core de 700 Mhz y solo 256 Mb de RAM con un costo cercano a los 35 dólares, a partir de ese año y basados en el éxito de su lanzamiento original ya se han generado al menos una docena de versiones diferentes de la placa original y ha aumentado notablemente sus características técnicas, al igual que el número de personas que la utilizan para un sinfín de proyectos diferentes entre los que están claramente las herramientas de seguridad informática

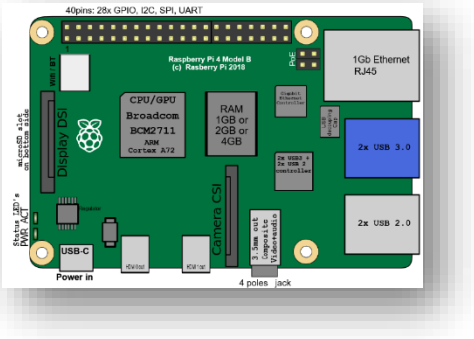

Figura 2. Raspberry Pi 4 Board. Fuente: https://www.raspberrypi.org/

La fundación Raspberry Pi soporta adicionalmente un par de proyectos más Code Club y CoderDojo que buscan fomentar que todos los niños puedan acceder a información sobre computación y sobre desarrollo de software, las SBC de Raspberry operan sobre el ecosistema de software libre y corren varias distribuciones de Linux, su sistema operativo oficial es Raspberry Pi OS llamado inicialmente Raspbian basada en la distribución Debian, el aumento progresivo en la capacidad de los SBC ha facilitado la incorporación de software de propósito general al sistema operativo de las Raspberry PI como Libre Office, y el soporte de herramientas de seguridad especializadas como IDS/IPS como Suricata, Snort, distribuciones orientadas a seguridad como Kali Linux, ParrotOS, e inclusive distribuciones como Debian tienen versiones de soporte para varias de las SMB como la Raspberry Pi

La versión más potente de la Raspberry Pi al día de hoy es la Raspberry Pi 4 que cuenta con procesador Quad Core a 1.8 Ghz, 8 Gb de memoria RAM, soporte para WiFi, Bluetooth, Gigabit Ethernet, puertos USB 2.0 y 3.0,

conector Mini HDMI, una ranura para tarjeta Micro-SD que se usa como almacenamiento para el sistema operativo y la data requerida por el mismo (soporta tarjetas de más de 2 Tb) y su módulo GPIO compatible con las versiones anteriores de Raspberry Pi. A raíz de la escasez de componentes electrónicos, ocasionada por la pandemia, género desabastecimiento del dispositivo y que por lo mismo se especulara mucho con sus precios en los sitios en los que aún se podía conseguir; al día de hoy no es económica, los paquetes que incluyen el SBC con 8 Gb de memoria RAM, una tarjeta Micro-SD de 64 Gb de memoria, un ventilador para disipar el calor que se conecta a los pines del GPIO, algunos disipadores de calor metálicos para la CPU, la RAM y el chip de Ethernet y una carcasa plástica que permita acomodar todo el paquete de manera cómoda se consigue por unos 175 dólares, en el sitio web de la fundación Raspberry Pi se pueden consultar literalmente cientos de proyectos de diversa índole, sin embargo, los proyectos asociados a ciberseguridad son pocos, dadas las capacidades de los SBC la instalación de soluciones de seguridad si bien no está incluida dentro de la lista oficial de proyectos soportados se puede evidenciar en muchos blogs y sitios de internet, la mayoría de los documentos muestran las instalaciones como ejercicios de pruebas y/o académicos, los resultados obtenidos demuestran que son una opción viable para realizar implementaciones en entornos de producción.

Las características físicas de estas placas (SBC) en su mayoría solo incluye un conector de red RJ-45 usualmente de 1 Gb y una interface Wi-Fi con soporte para 802.11 b/g/n/ac en el caso de la Raspberry PI modelo B, en otras placas el soporte de hardware es muy similar, con esta consideración varias de las herramientas en cuya función se hace recepción del tráfico por una interface y entrega luego del análisis y/o modificaciones del misma en la otra, hay que considerar entonces que el proceso de entrega de tráfico no puede ser superior a las velocidades de soporte de estas interfaces porque de lo contrario se pueden generar cuellos de botella en las funciones de las herramientas de seguridad a implementar.

5. Herramientas de seguridad

Si bien existe una amplia lista de herramientas de seguridad informática open source que se pueden descargar y utilizar de manera exitosa sobre placas (SBC), y que se pueden configurar sobre la versión del sistema operativo que soporte la SBC, es necesario verificar que la herramienta seleccionada este soportada por la SMB y el sistema operativo que esta soporte, en particular con la que estemos trabajando, algunas herramientas en razón a sus requerimientos pueden no ser candidatas a instalar o requerir configuraciones que no sean sencillas de implementar y complejas de soportar, por lo que es

mejor seleccionar alguna herramienta cuya compatibilidad con la SMB esté garantizada, la lista de herramientas que pueden apoyar a las pymes consideraría al menos las siguientes:

Tabla 1. Lista de herramientas propuesta

Herramienta	Descripción	Nombre
Firewall	Controla el trafico de red	Iptables, pfsense
Antivirus	Detecta, previene y elimina malware virus, gusanos, troyanos en sistemas y redes	Bitdefender, Avira
Sistema de Detección y prevención de Intrusos (IDS/IPS)	Monitorea y bloquea en la red actividades sospechosas y/o maliciosas	Snort. Suricata
Analisis de registros	Examina y analiza los registros de eventos del sistema	ELK Stack, LOGalyze
Escáner de Vulnerabilidades	Identifica y evalúa vulnerabilidades en sistemas	OpenVAS, Nessus

Fuente: propia.

La anterior no es una lista exhaustiva de herramientas de seguridad informática open source pero la mayoría de ellas se pueden instalar y configurar en las SBC más populares, en cuanto al requerimiento de número de interfaces, para herramientas que funcionen en modo monitoreo como un IDS/IPS solo requeriría una interface, aunque si se va a colocar en modo in-line si se requerirían las dos interfaces, en herramientas que solo necesitan la interface RJ-45 como el escáner de vulnerabilidades, hasta herramientas en donde el número de interfaces requeridas puede ser mayor como en un firewall en donde sería conveniente al menos dos interfaces, para este caso si las capacidades de rendimiento que ofrecen las placas SMB se pueden conectar interfaces de red a los puertos USB disponibles para con ello aumentar el número según sea necesario, para cada una de estas herramientas se debe analizar el uso que se le va a dar y seleccionar la herramienta de seguridad apropiada

5.1 Soluciones de firewall

Las herramientas de firewall cuyas funciones principales son realizar enrutamiento y proveer capacidades de control de tráfico entre redes, se pueden implementar en placas SBC, usualmente este tipo de soluciones requieren varias interfaces, sin embargo en el contexto de una pyme que

debería tener menores requerimientos de rendimiento y capacidades de procesamiento la solución debería funcionar correctamente, con dos de las interfaces de red (RJ-45 e Inalámbrica) disponibles, con ellas puede ser suficiente para atender los requerimientos o de ser necesario se puede habilitar otra interface en uno de los puertos USB, las principales soluciones open source son:

Tabla 2. Herramientas de firewall

Firewall	Descripcion	Caracteristicas
OPNsense	Basado en PFSense, firewall y enrutamiento	Interface web, filtro por estado, IDS, soporte VPN, balanceo de carga, gestion unificada de amenazas
pfSense	Firewall y enrutamiento basado en FreeBSD	Interface Web, filtro por estado, IDS, soporte VPN, Balanceo de cargas, reportes
IPFire	Enrutamiento y firewall flexible y modular	Filtrado de paquetes, proxy web, filtrado de paquetes, IDS, QoS

Fuente: propia.

Se debe considerar que las soluciones de open source ofrecen unas capacidades básicas similares, pero que pueden tener diferencias en cuanto a la implementación de las interfaces web de administración y configuración e incluir algunas capacidades específicas dependiendo de la solución, por lo que la selección de la solución debe realizarse evaluando las necesidades específicas de cada pyme.

5.2 Soluciones de IDS/IPS

Las herramientas de IDS/IPS cuyas funciones principales son realizar análisis y detección de tráfico anómalo para descartarlo (drop) o en el caso de los IPS para poder tomar acciones automáticas relacionadas con el comportamiento detectado como alertarlo, o automáticamente generarle reglas al firewall para bloquear el tráfico.

Tabla 3. Herramientas de IDS/IPS

Características	Snort	Suricata
Número de reglas	Más de 11,000	Más de 40,000
Velocidad de procesamiento	5-10 Gbps	10-20 Gbps
Soporte de protocolos	TCP, UDP, ICMP, HTTP, DNS, FTP, SMTP, SSH, SIP, SSL, entre otros.	TCP, UDP, ICMP, HTTP, DNS, FTP, SSH, SIP, SSL, entre otros.
Funcionalidades	Detección de intrusiones, prevención de intrusiones, registro de eventos, captura de paquetes, análisis de tráfico, entre otros.	Detección de intrusiones, prevención de intrusiones, registro de eventos, captura de paquetes, análisis de tráfico, análisis de malware, entre otros.
Lenguajes de reglas	Snort y Emerging Threats open	Suricata y Emerging Threats open
Flexibilidad	Limitada	Mayor
Comunidad	Grande y activa	Grande y activa
Licencia	GPLv2	GPLv2

Fuente: propia.

En las configuraciones donde la solución de IDS/IPS se configura en modo in-line se requiere de dos interfaces para que su funcionamiento sea más fluido, en las configuraciones en donde está en modo monitoreo el uso de una sola de las interfaces es suficiente.

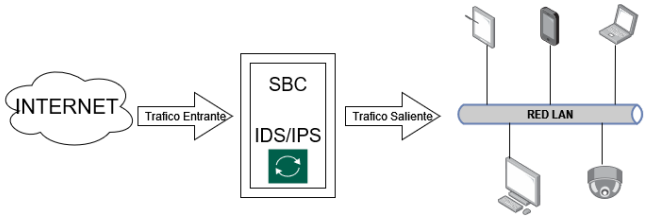

Figura 3. Diagrama de configuración IDS/IPS. Fuente: propia.

En las configuraciones donde la solución de IDS/IPS se configura en modo in-line se requiere de dos interfaces para que su funcionamiento sea más fluido, en las configuraciones en donde está en modo monitoreo el uso de una sola de las interfaces es suficiente.

Referencias

Almanza, A. (s.f.). XXII Encuesta Nacional de Seguridad Informática. (s.f.). Sistemas. https://sistemas.acis.org.co/index.php/sistemas/article/view/186/146

Bancoldex (s.f.) ¿Qué es una pyme? (s.f.). https://www.bancoldex.com/que-es-una-pyme-1338

DANE (s.f.). Encuesta de micronegocios. DANE. https://www.dane.gov.co/index.php/estadisticas-por-tema/mercado-laboral/micronegocios

Dirección Nacional de Planeación. (01 de julio de 2020). Documento Conpes 3995. https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3995.pdf

Dirección Nacional de Planeación. (14 de julio de 2011). Documento Conpes 3701. https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3701.pdf

IBM-Security. (2019). Cost of Data Breach Report. https://www.ibm.com/downloads/cas/3R8N1DZJ

IoT Analytics. (s.f.). State of IoT 2022: Number of connected IoT devices growing 18% to 14.4 illion globally. IoT Analytics. https://iot-analytics.com/number-connected-iot-devices/

Senado de la República. (26 de enero de 2023). Colombia requiere de una Agencia Nacional de Ciberseguridad. https://www.senado.gov.co/index.php/el-senado/noticias/4314-colombia-requiere-de-una-agencia-nacional-de-ciberseguridad