Nombre de la materia:
Fundamento de telecomunicaciones

Nombre de la licenciatura:
SISTEMAS COMPUTACIONALES

Nombre del alumno(a):
ALAN GERARDO GIJON AGOSTO

Número de control:
18530390

Nombre de la tarea: Investigar sobre SIEM e IDS/IPS

Unidad #: nombre de la unidad:

Nombre del profesor(a):
ING. ISMAEL JIMENEZ SANCHEZ

Fecha:

IDS/IPS

Los sistemas TI atesoran un gran caudal de información sobre nuestras organizaciones. Desde contenidos corporativos -como la contabilidad-, a bases de datos sobre clientes, documentos técnicos confidenciales… en esencia, el ADN de la propia empresa. La actividad de cada compañía descansa sobre importantes volúmenes de información, de cuya integridad puede depender hasta la misma existencia de la firma. Por ello, debemos esforzarnos en proteger nuestro principal activo con todos los medios que tengamos al alcance. Hoy os contamos qué son los sistemas de detección y prevención IDS e IPS y cuál es su función.

IDS

IDS (Intrusion Detection System) o sistema de detección de intrusiones: es una aplicación usada para detectar accesos no autorizados a un ordenador o a una red, es decir, son sistemas que monitorizan el tráfico entrante y lo cotejan con una base de datos actualizada de firmas de ataque conocidas. Ante cualquier actividad sospechosa, emiten una alerta a los administradores del sistema quienes han de tomar las medidas oportunas. Estos accesos pueden ser ataques esporádicos realizados por usuarios malintencionados o repetidos cada cierto tiempo, lanzados con herramientas automáticas. Estos sistemas sólo detectan los accesos sospechosos emitiendo alertas anticipatorias de posibles intrusiones, pero no tratan de mitigar la intrusión. Su actuación es reactiva.

IPS

IPS (Intrusion Prevention System) o sistema de prevención de intrusiones: es un software que se utiliza para proteger a los sistemas de ataques e intrusiones. Su actuación es preventiva. Estos sistemas llevan a cabo un análisis en tiempo real de las conexiones y los protocolos para determinar si se está produciendo o se va a producir un incidente, identificando ataques según patrones, anomalías o comportamientos sospechosos y permitiendo el control de acceso a la red, implementando políticas que se basan en el contenido del tráfico monitorizado, es decir, el IPS además de lanzar alarmas, puede descartar paquetes y desconectar conexiones.

Muchos proveedores ofrecen productos mixtos, llamándolos IPS/IDS, integrándose frecuentemente con cortafuegos y UTM (en inglés Unified Threat Management o Gestión Unificada de Amenazas) que controlan el acceso en función de reglas sobre protocolos y sobre el destino u origen del tráfico.

Ventajas y desventajas de cada herramienta

IDS

La principal ventaja de un sistema IDS es que permite ver lo que está sucediendo en la red en tiempo real en base a la información recopilada, reconocer modificaciones en los documentos y automatizar los patrones de búsqueda en los paquetes de datos enviados a través de la red. Su principal desventaja es qué estas herramientas, sobre todo en el caso de las de tipo pasivo, no es están diseñadas para prevenir o detener los ataques que detecten, además son vulnerables a los ataques DDoS que pueden provocar la inoperatividad de la herramienta.

IPS

Las ventajas de un IPS son:

- escalabilidad al gestionar multitud de dispositivos conectados a la misma red;
- protección preventiva al comprobarse de forma automatizada comportamientos anómalos mediante el uso de reglas prefijadas;
- fácil instalación, configuración y administración al estar disponibles multitud de configuraciones predefinidas y centralizar en un punto su gestión, aunque puede ser contraproducente para su escalabilidad;/
- defensa frente a múltiples ataques, como intrusiones, ataques de fuerza bruta, infecciones por malware o modificaciones del sistema de archivos, entre otros;
- aumento de la eficiencia y la seguridad de la prevención de intrusiones o ataques a la red.

Entre sus desventajas, destacan los efectos adversos que pueden producirse en el caso de que se detecte un falso positivo, si por ejemplo se ejecuta una política de aislamiento de las máquinas de la red o en el caso de que se reciban ataques de tipo DDoS o DoS que pueden provocar su inutilización.

¿Por qué es aconsejable contar con alguna de estas herramientas?

Estas herramientas permiten a las empresas enfrentarse, ya sea de forma pasiva (automatizada) o activa a las amenazas que puedan afectar al buen funcionamiento de los sistemas, como pueden ser redes de comunicaciones, dispositivos o sensores IoT, ya que en menor o mayor medida ayudan a detectar y neutralizar las intrusiones, amenazas o comportamientos sospechosos que ponen en riesgo la ciberseguridad de la empresa. Dicho de otra manera, son un paso natural en la evolución de la ciberseguridad.

Bibliografía:

https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips

https://puntinformatic.com/sistemas-de-deteccion-y-prevencion-ids-e-ips/#:~:text=Tanto%20los%20Sistemas%20de%20Detecci%C3%B3n,datos%2C%20para%20detectar%20patrones%20sospechosos.