Revista Cubana de Ciencias Informáticas
Vol. 9, No. 3, Julio-Septiembre, 2015
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 18- 32

Tipo de artículo: Artículo original
Temática: Seguridad informática
Recibido: 18/05/2015 | Aceptado: 25/05/2015

Marco de trabajo para la gestión centralizada de trazas de seguridad usando herramientas de código abierto

Framework for centralized security logs management using open source tools

Joelsy Porven Rubier [1*], Raydel Montesino Perurena [1]

[1] Universidad de las Ciencias Informáticas, Carretera a San Antonio de los Baños, km 2 ½, Torrens, Boyeros, La Habana, Cuba. CP.: 19370.

[*] Autor para correspondencia: jporven@uci.cu

Resumen

La gestión de trazas en los sistemas informáticos es un proceso fundamental para garantizar la seguridad. La gran mayoría de software, hardware y dispositivos de red, poseen mecanismos para generar registros del estado de su funcionamiento. Es de gran importancia conocer los accesos realizados, u otros eventos que permiten determinar el comportamiento de un sistema en un período de tiempo. Las trazas se generan en diferentes formatos lo que hace difícil su procesamiento. La gestión de trazas requiere de sistemas que procesen y normalicen la gran variedad de formatos existentes. También es fundamental definir mecanismos de transporte, planeación y ejecución, sistemas de almacenamiento eficientes en cuanto la utilización de espacio y herramientas para la búsqueda y detección de patrones. En el presente artículo se expone un análisis de las principales regulaciones y normas existentes en cuanto a los requerimientos que debe tener un sistema de gestión centralizado de trazas. Se propone un marco de trabajo y una arquitectura centralizada con los componentes necesarios. Como resultado del análisis desarrollado se evalúan las herramientas de software libre para la implementación de la arquitectura propuesta.

Palabras clave: trazas, syslog, seguridad, gestión

Abstract

Managing logs in computer systems are a fundamental process to ensure security. The vast majority of software, hardware and network devices possess mechanisms for generating records of state operation. It is very important to know system accesses, or other events that should determine how have performed its operation in a time period. Logs

Revista Cubana de Ciencias Informáticas
Vol. 9, No. 3, Julio-Septiembre, 2015
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 18- 32

are generated in different formats making it difficult to process. Log management systems require that process and standardize the variety of existing formats. It is also essential to define mechanisms of transport, planning and implementation of storage systems as efficient space utilization and tools for searching and pattern detection. In this paper an analysis of the principal regulations and standards regarding the requirements that must have a centralized management system logs are exposed. A framework and a centralized architecture with the components required are proposed. As a result of the analysis developed a free software tools for the implementation of the proposed architecture are evaluated.

Keywords: *log, management, syslog, security*

Introducción

La gestión de trazas en los sistemas informáticos es esencial a la hora de garantizar la seguridad. Los sistemas y dispositivos de hardware dentro de una red, incluyen mecanismos para generar registros del estado de su funcionamiento, accesos realizados u otros eventos, que en su conjunto permiten conocer su comportamiento en el tiempo.

Desde el punto de vista de la seguridad, es fundamental poder establecer la trazabilidad de un suceso determinado. Esto permite determinar las causas de un incidente mediante el análisis forense o detectarlo en el momento de su ocurrencia. De mayor importancia es poder obtener información de las trazas generadas que permitan accionar de forma proactiva.

Los procesos de gestión de trazas de los sistemas informáticos, aunque están presentes en las principales regulaciones y normas existentes, siguen teniendo varias dificultades en su puesta en práctica. Muestra de ello son los datos que aporta el informe de la compañía Verizon en 2012 (Baker, et al. 2012). El documento refleja que solo el 8 % de las grandes compañías (más de 1000 empleados) y un 1 % de resto, detectó la ocurrencia de los incidentes mediante el análisis de trazas y eventos de seguridad cuando en el 84 % de los casos estaba disponible la evidencia en las trazas. También se plantea como resultado, que la detección de incidentes demora en la mayoría de los casos analizados, semanas, meses e incluso años. Actualmente sigue existiendo una brecha bastante grande entre los tiempos de compromiso y el tiempo en que logra descubrirse el ataque o pérdida de datos(Verizon, 2014).

El proceso de gestión de trazas requiere de variantes que integren la gran cantidad de formatos existentes. Se deben definir mecanismos de transporte que no tengan una influencia considerable en el tráfico de la red, de planeación, ejecución así como mecanismos de almacenamiento eficientes en cuanto la utilización de espacio y herramientas para la búsqueda y detección de patrones. En el presente artículo se expone un análisis de las principales regulaciones y

normas existentes en cuanto a los requerimientos que debe tener un sistema de gestión centralizado de trazas. Se propone un marco de trabajo para la gestión centralizada de trazas así como la arquitectura y componentes necesarios como resultado del análisis desarrollado. Se evalúan las herramientas de software de código abierto necesarias para la implementación de la arquitectura propuesta.

Materiales y métodos o Metodología computacional

En el presente trabajo se utilizó como métodos de investigación:

Inductivo-deductivo: Analizando las principales regulaciones, normas y guías de seguridad consultadas en la bibliografía para resumir y hacer una síntesis de los elementos fundamentales que permitan elaborar una propuesta y obtener las conclusiones necesarias.

Resultados y discusión

Referencias a la gestión de trazas en estándares, guías y documentos de buenas prácticas de seguridad

Las trazas generadas por los sistemas de hardware y software tienen una importancia fundamental en el proceso de gestión de la seguridad de la información. Dentro de los principales documentos está la guía de buenas prácticas de la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC) ISO/IEC 27002 como parte de la norma certificable ISO/IEC 27001. La sección 12, seguridad de las operaciones, se dedica al tratamiento de las trazas y la subsección 12.4, registro y monitoreo, contiene cuatro controles asociados(ISO y Std,2005).

Estos son:

- Registro de eventos, con 15 tipos principales a registrar.
- Seguridad de las trazas almacenadas en cuanto a modificación o eliminación.
- Registro de las actividades de los administradores de sistemas
- Sincronización de tiempo

El Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (PCI DSS por sus siglas en inglés) desarrollado por el "*Payment Card Industry Security Standards Council*" (PCI SSC) Propone 12 requerimientos a cumplir. El décimo requisito con siete elementos a tener en cuenta asociados a: registro de acceso de forma

individual, registro automático de eventos, campos que deben contener los eventos, sincronización de tiempo, seguridad de las trazas, revisión periódica y retención(Council, 2010).

La división de seguridad del Instituto Nacional de Estándares y Tecnologías de EEUU (NIST) desarrolla un conjunto de publicaciones especiales conocidas como Serie 800, ampliamente adoptadas por la comunidad de especialistas de seguridad. El documento SP 800-53, Controles de seguridad recomendados para los sistemas de información y organizaciones federales, dedica 14 controles específicos a la auditoría y gestión de trazas(NIST, 2007).

Un estudio realizado por un grupo de expertos de seguridad, publicado bajo el título "*Twenty Critical Controls for Effective Cyber Defense: Consensus Audit Guidelines*" (CAG), lo integran 20 controles técnicos que son críticos e indispensables en un sistema de seguridad informática. El control 14: monitoreo, mantenimiento y análisis de las trazas de auditoría; propone 11 acciones concretas sobre el monitoreo y análisis de trazas(CSIS, 2013).

El grupo de seguridad de Comunicaciones electrónicas (CESG) del Reino Unido, publica una serie de documentos y guías de buenas prácticas de obligatorio cumplimiento para instituciones estatales. Compañías líderes en el área de la gestión de trazas y de eventos de seguridad, ofrecen productos que cumplen con la guía GPG13 que pertenece a esta serie. GPG13 consta de 12 aspectos para garantizar el monitoreo continuo de protección. La implementación de cada uno de los aspectos descritos está directamente relacionada con la capacidad de gestión de trazas(AccelOps, 2013).

En Cuba, de obligatorio cumplimiento para todas las entidades, está la resolución 127 de 2007 del Ministerio de la Informática y las Comunicaciones (MIC) actualmente Ministerio de las Comunicaciones (MICOM). La resolución cuenta con 100 artículos. La sección octava del Capítulo III trata sobre la seguridad de redes con tres artículos. Concretamente, los artículos 58 inciso b, 62 inciso b y 83 inciso b tratan sobre la generación, revisión periódica y específicamente el registro de las conexiones remotas(MIC, 2007).

De las guías y documentos de buenas prácticas descritas se pueden extraer tres categorías asociadas a la gestión de trazas. Una categoría general asociada a los componentes necesarios en la implementación de un sistema de gestión de trazas, los registros de trazas de mayor importancia para la seguridad de los sistemas monitorizados y a un nivel más profundo, los campos que deben contener estos registros. En la Figura 1 se representa cada una de las categorías.

Por otra parte, se puede destacar que la ISO/IEC 27002 hace mayor énfasis en los registros de eventos. PCI DSS propone explícitamente los campos que deben contener los registros de eventos. El resto está orientado principalmente a los componentes que debe conformar un sistema de gestión de trazas.

Revista Cubana de Ciencias Informáticas
Vol. 9, No. 3, Julio-Septiembre, 2015
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 18- 32

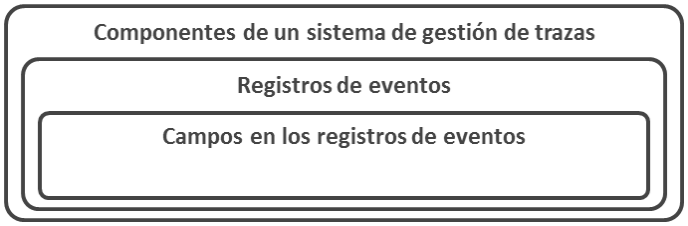

Figura 1. Categorías asociadas a la gestión de trazas

Componentes y principales eventos que deben ser registrados

Tomando como base un grupo de los principales documentos existentes, en cuanto a la gestión de seguridad y buenas prácticas, se muestra en la Tabla 1 una síntesis de los componentes asociados a la gestión de trazas que se tienen en cuenta por cada documento analizado.

Para medir la importancia de cada recomendación se revisó su aparición, obteniendo como resultado cuáles tenían mayor presencia y por tanto serían las más importantes a tener en cuenta.

En la Figura 2 se muestra el resultado y cómo la generación, revisión periódica, tener una fuente de tiempo confiable, qué información deben tener las trazas que se van a almacenar, por cuanto tiempo se van a conservar y su seguridad; deben ser los aspectos primarios a considerar.

Tabla 1. Síntesis de los principales componentes por cada una de las guías de buenas prácticas y estándares fundamentales en cuanto a la gestión de trazas

Componentes	**27002**	**PCIDSS**	**800-53**	**CAG**	**GPG13**	**MIC 127**
Generación y registro de trazas	x	x	x	x	x	x
Sincronización de tiempo	x	x	x	x	x	-
Seguridad de las trazas	x	x	x	x	-	-
Revisión periódica de las trazas	x	x	x	x	x	x
Retención	-	x	x	x	-	x
Políticas y procedimientos de auditoría	-	-	x	-	-	-
Definir eventos auditables	-	-	x	-	-	-
Contenido de los registros de eventos	x	x	x	x	-	-
Capacidad de almacenamiento	-	-	x	x	-	-
Respuesta a fallos del sistema de auditoría	-	-	x	-	x	-
Reducción de trazas	-	-	x	x	-	-
No repudio	-	-	x	x	-	-

Revista Cubana de Ciencias Informáticas
Vol. 9, No. 3, Julio-Septiembre, 2015
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 18- 32

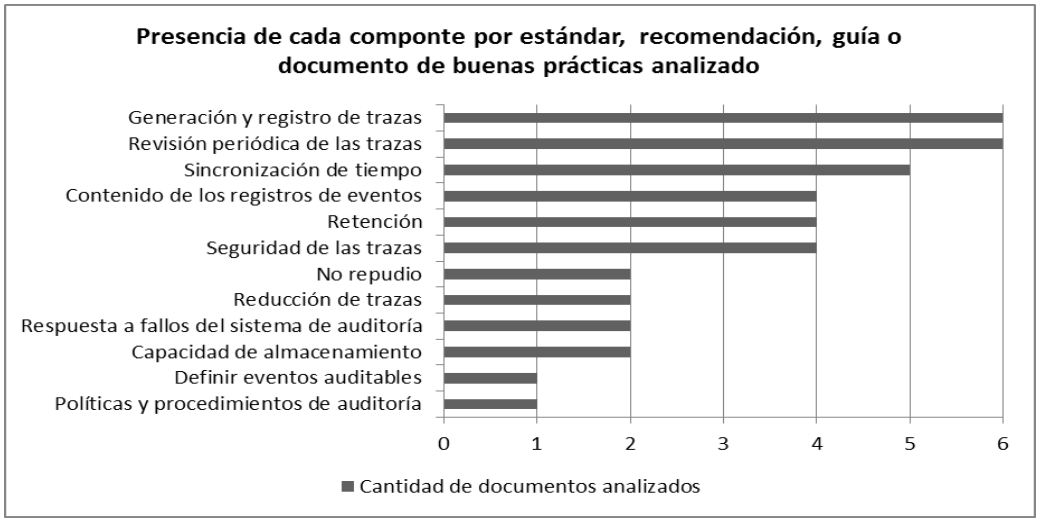

Figura 2. Presencia de cada componente por guía o norma de buenas prácticas de seguridad analizada

Una síntesis de la información qué debe ser registrada y almacenada para su análisis y presentación de reportes se muestra en la Tabla 2. Se agrupa en nueve tipos de registros de eventos genéricos, presentes explícitamente al menos en uno de los documentos analizados.

Tabla 2. Principales registros de eventos y su presencia en cada una de las principales guías y estándares

Registro de evento	**Mapeo contra las principales regulaciones y guías de buenas prácticas**
Acciones con privilegios administrativos	27002; PCIDSS; CAG
Acceso a las trazas	PCIDSS
Monitoreo de sesiones	NIST 800-53, GPG13
Eventos satisfactorios y fallidos de usuarios, aplicaciones y sistemas	PCIDSS;800-53;CAG;GPG13;27002
Creación, modificación y borrado de objetos del sistema	PCIDSS;27002
Monitoreo de fuga de información	NIST 800-53;GPG13
Registro de conexiones remotas	CAG;GPG13;127/2007
Registro de trazas tráfico de red	27002;GPG13
Eventos Críticos	GPG13

Cada registro de evento idealmente debe proveer un conjunto de información que permita obtener una trazabilidad, lo más completa posible, del evento ocurrido. Un evento debe proveer la información necesaria para responder cinco preguntas que se conocen por su terminología en inglés como las cinco W's(Chuvakin, Schmidt y Phillips, 2012).

1. ¿Qué pasó?
2. ¿Cuándo pasó?
3. ¿Dónde pasó?
4. ¿Quién está involucrado?
5. ¿Cuál fue la fuente de origen?

Dentro de las guías analizadas, PCI DSS detalla explícitamente qué campos deben tener los registros de eventos. En la ISO/IEC 27002 junto con los eventos que se deben registrar se mencionan algunos de los campos que deben contener las trazas. La guía del NIST 800-53 dentro de la familia de controles, auditoria y contabilidad, incluye el control AU-3 contenido de los registros de eventos. La Tabla 3 muestra un resumen de los eventos propuestos y su relación con la información necesaria para garantizar la trazabilidad de un evento.

Tabla 3. Asociación de los campos de registros de eventos a los que se hace referencia explícitamente en la guías ISO/IEC 2002 y PCI DSS junto con la información que proveen

Campos	ISO/IEC 27002	PCI DSS	Responde a
Identificación de usuario	x	x	¿Quién está involucrado?
Tipo de eventos. Satisfactorios y fallidos	-	x	¿Qué pasó?
Fecha y hora	x	x	¿Cuándo pasó?
Fuente donde se generan los eventos	x	x	¿Cuál fue la fuente de origen?
Nombre del objeto afectado	-	x	¿Dónde pasó?
Direcciones de red y protocolos	x	-	¿Quién está involucrado?

El documento del NIST SP800-92(Kent y Souppaya, 2006) está dedicado completamente a la gestión de trazas. En cinco secciones, trata las necesidades y retos de las organizaciones, arquitectura y funciones así como las recomendaciones para la elaboración de políticas y los procesos a llevar a cabo en las operaciones de gestión de trazas.

SP800-92 propone una infraestructura de gestión de trazas compuesta por tres capas:

- Generación de trazas: Es donde van a estar los servidores estaciones de trabajo y dispositivos que generan los datos.
- Análisis y almacenamiento de trazas: Esta capa está compuesta por uno o más servidores de trazas que reciben los datos, ya sea en tiempo real o mediante aplicaciones que envían las trazas cada cierto tiempo.
- Monitoreo de trazas: Contiene las consolas para la revisión, análisis automático y generación de reportes.

La guía plantea la implementación en tres etapas como se muestra en la Figura 3.

Revista Cubana de Ciencias Informáticas
Vol. 9, No. 3, Julio-Septiembre, 2015
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 18- 32

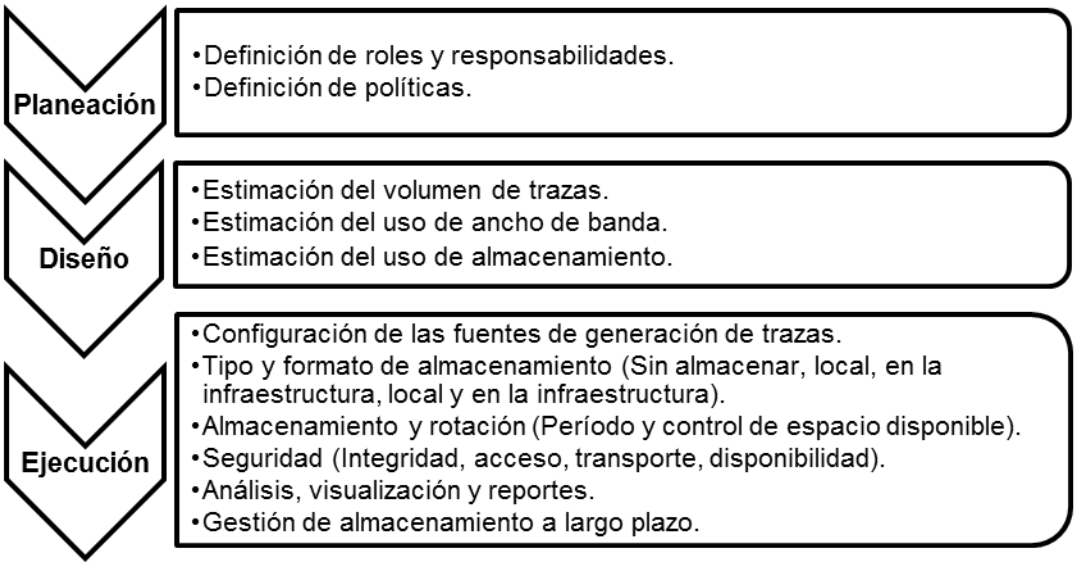

Figura 3. Etapas de implementación de un sistema de gestión centralizado de trazas siguiendo la guía del NIST SP800-92

El documento SP 800-92 contiene la descripción completa de los pasos necesarios para el desarrollo de una infraestructura de gestión de trazas.

Aunque la guía cubre los procesos clásicos de la gestión de trazas, las redes, los sistemas y la seguridad han ido evolucionando aceleradamente. Nuevos actores han tomado protagonismo; como la computación en la nube, la gestión de grandes volúmenes de datos y la seguridad como servicio. El documento analizado no ha sido objeto de una actualización desde su publicación en 2006. Como un documento generalizador, no plantea una arquitectura de despliegue donde se integren cada uno de los componentes en una solución aplicada. De igual forma, trata las fuentes de generación de trazas haciendo una clasificación global, no propone una selección de eventos según su importancia, resumiendo solamente una lista genérica de software de seguridad así como la información que debe ser tomada en cuenta en cuanto a los sistemas operativos y aplicaciones de usuario.

Otro elemento importante, es el análisis de las herramientas y recursos propuestos en el apéndice C; nuevos formatos de trazas y aplicaciones de software que no se mencionan, han sido desarrollados y ocupan un rol importante en el proceso de gestión de trazas.

Del análisis realizado, donde se sintetizan los eventos principales, su importancia y los registros de mayor prioridad que deben ser recolectados así como las recomendaciones de la guía SP 800-92, se resumen los componentes fundamentales para un sistema integrado por un conjunto de elementos lógicos y software que gestione centralizadamente las trazas de seguridad.

Revista Cubana de Ciencias Informáticas
Vol. 9, No. 3, Julio-Septiembre, 2015
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 18- 32

Marco de trabajo para la gestión de trazas de seguridad

El marco de trabajo lo integran los procesos de planeación, diseño y ejecución necesarios para poner en operación una arquitectura de gestión de trazas. Como primer componente se requiere de definir políticas roles y responsabilidades que sustenten la ejecución de una arquitectura centralizada. La arquitectura propuesta debe estar correctamente dimensionada mediante el cálculo de los parámetros para la estimación del volumen de trazas, almacenamiento y uso de ancho de banda.

La arquitectura se compone de cuatro capas:

- Generación de trazas
- Transporte
- Análisis y almacenamiento
- Monitoreo

Dentro de las funciones generales están: Las acciones de configuración necesarias para el filtrado de los eventos generados, las acciones de análisis que permiten la normalización, conversión y reducción de los eventos recibidos centralmente y la agregación en una localización central mediante la compresión e indexado de las trazas.

Una vez almacenados los registros, una aplicación de monitoreo se encarga de brindar las funciones de visualización y generación de variables estadísticas asociadas a las trazas que se presentan al analista de seguridad.

En cada uno de los procesos descritos se tienen en cuenta un conjunto de configuraciones de seguridad que incluyen:

- Sincronización usando un servidor de tiempo para mantener sincronizado las diferentes fuentes de generación almacenamiento y sistemas de monitoreo de trazas.
- Uso de buffers de almacenamiento temporal para evitar la pérdida de eventos ante un corte de transmisión, recepción o problemas con el canal de red.
- Uso de canales cifrados para la transmisión de datos (TLS) y protocolos seguros para la transmisión (RELP, TCP) siempre que sea posible.
- Generación de funciones resumen y chequeo de integridad de los ficheros de trazas almacenados.
- Monitoreo del acceso a los ficheros de trazas registrando las operaciones, lectura, escritura, creación o modificación que puedan realizarse a nivel de sistema de ficheros.

Revista Cubana de Ciencias Informáticas
Vol. 9, No. 3, Julio-Septiembre, 2015
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 18- 32

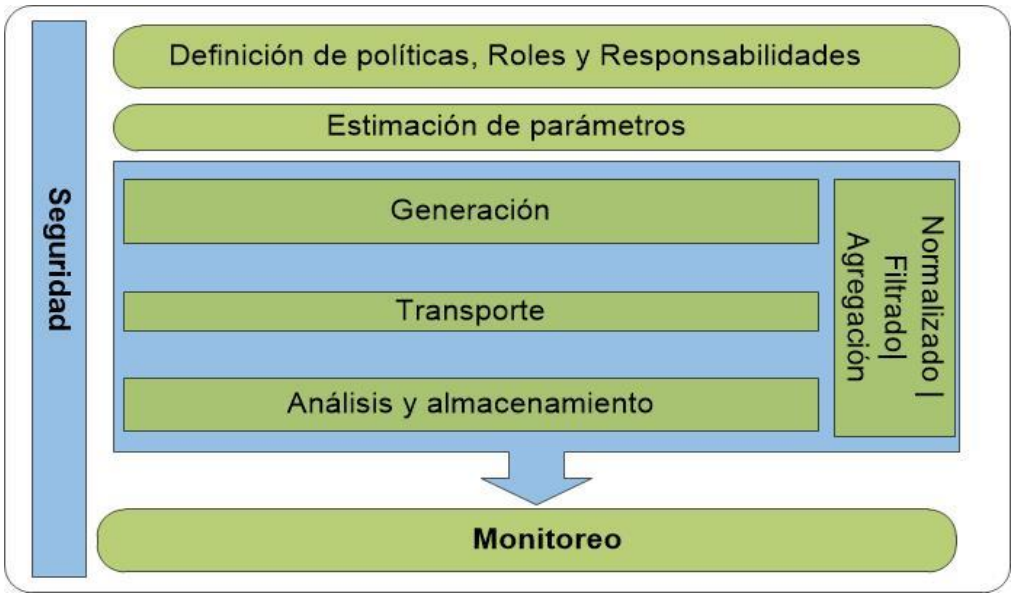

Figura 4. Marco de trabajo para la gestión centralizada de trazas de seguridad

En el marco de trabajo propuesto, cada proceso para su ejecución requiere de un grupo de herramientas que sean capaces de integrarse de manera satisfactoria. El uso de varias herramientas y su instalación requiere del manejo de múltiples ficheros de configuración. Para esto se propone que la gestión de configuración se realice mediante el uso de SaltStack. SaltStack permite la gestión centralizada y la configuración, instalación de software y ejecución de comandos en un gran número de computadores, servidores, estaciones de trabajo y dispositivos de forma simultánea. Una misma configuración puede ser aplicada a múltiples arquitecturas y sistemas operativos mediante la interpretación de plantillas genéricas (Craig Sebenik, 2015).

El sistema se estructura mediante la arquitectura que se muestra en la Figura 5. Está compuesto por las herramientas que permiten manejar los 9 tipos de eventos descritos junto con el resto de los componentes necesarios para implementar el marco de trabajo propuesto. Se presenta una solución de gestión de trazas apoyada en herramientas de software libre que permite gestionar todo el proceso de recolección, transporte, almacenamiento, generación de reportes sincronización de tiempo y gestión de configuración.

La

Tabla **4** describe de forma general cada una de las herramientas que se utilizan en la arquitectura propuesta.

Revista Cubana de Ciencias Informáticas
Vol. 9, No. 3, Julio-Septiembre, 2015
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 18- 32

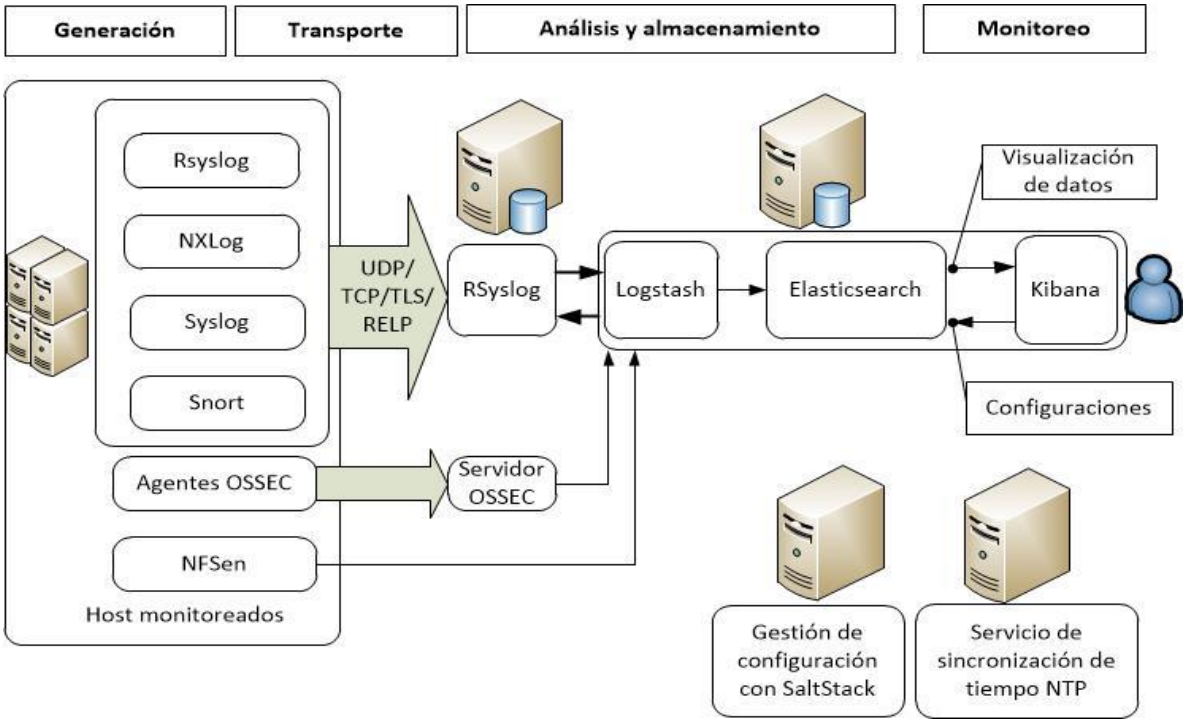

Figura 5. Arquitectura de despliegue para la gestión centralizada de trazas de seguridad

Tabla 4. Selección de herramientas que componen la arquitectura propuesta

Software	**Descripción**
Rsyslog	Software para el procesamiento de trazas en los sistemas Linux. Viene como opción predeterminada en la mayoría de las distribuciones. Recolecta las trazas del sistema permitiendo la recolección, almacenamiento, filtrado, reducción y retransmisión de los eventos procesados.
NXLog	Software para el procesamiento de trazas. Recolecta las trazas de diversas fuentes. Implementa múltiples mecanismos de filtrado, permite correlacionar eventos, permite el almacenamiento y retransmisión en múltiples formatos y es multiplataforma estando disponible para Linux, UNIX, Windows y Android(Botond Botyanszki, 2009).
Snort	Sistema de Detección de Intrusiones de Red (NIDS, por sus siglas en inglés) con capacidad de análisis y registro de paquetes en tiempo real(Baker, Esler y Alder, 2007).
OSSEC	OSSEC es un Sistema de Detección de Intrusiones de Host (HIDS, por sus siglas en ingles) con capacidades de análisis de trazas, chequeo de integridad de ficheros, monitoreo de políticas, detección de rootkits, generación de alertas en tiempo real y respuesta activa(Bray, Cid y Hay, 2008).

Auditd	Mecanismo en los sistemas Unix/Linux para registrar información relevante a la seguridad basado en reglas(Miclea, 2012).
Logstash	Herramienta para el manejo de trazas. Permite la recolección en múltiples formatos, gran cantidad de funciones de filtrado, y múltiples formatos de salida(Gormley y Tong, 2014).
Elasticsearch	Motor distribuido de análisis y búsqueda. Se integra con la mayoría de los lenguajes más populares y se maneja casi completamente mediante una API RESTful usando JSON sobre HTTP. Actualmente se integran Logstash + Elasticsearch + Kibana para proveer una solución completa de análisis de trazas conocida como ELK(Gormley y Tong, 2014).
Kibana	Sistema analítico que permite realizar y visualizar múltiples tipos de búsquedas en datos almacenados sobre Elasticsearch(Gormley y Tong, 2014).
NTP	Protocolo designado para sincronizar la hora de las computadoras y dispositivos conectados a la red(Rybaczyk, 2005).
Nfsen	Nfsen lo componen un conjunto de herramientas en línea de comandos que permiten capturar tráfico netflow. Lo componen nfcapd, nfdump, nfprofile, nfreplay, nfclean.pl, ft2nfdump(Fry y Nystrom, 2009).
SaltStack	SaltStack permite la gestión centralizada y la configuración, instalación de software y ejecución de comandos en un gran número de computadores, servidores, estaciones de trabajo y dispositivos de forma simultánea. Una misma configuración puede ser aplicada a múltiples arquitecturas y sistemas operativos mediante la interpretación de plantillas genéricas (Craig Sebenik 2015)

Dentro de las herramientas descritas es importante señalar la presencia de auditd. Esta herramienta no es necesario instalarla, viene preinstalada con el sistema operativo para el caso de Windows si incluye la misma funcionalidad dentro de las políticas del sistema.

La arquitectura mostrada envía los eventos hacia un servidor central de Syslog, después de ciertos niveles de procesamiento y reducción envía las trazas hacia Logstash para un segundo nivel de filtrado, normalización, indexado y almacenamiento en el sistema de indexado Elasticsearch. Una vez almacenadas se puede realizar y mostrar los resultados de distintos tipos de búsquedas usando Kibana. Las trazas almacenadas pueden tener indicadores como nombres de índices diferentes. Kibana puede ser configurado con múltiples paneles de mando (Dashboard) asociados a los datos almacenados o a parte de estos. Las configuraciones se guardan en Elasticsearch. En el caso del procesamiento de tráfico Netflow se envía directamente hacia Logstash y para Ossec se usa un servidor central donde se recolectan las alertas recibidas antes de enviarlas.

Otra de las características fundamentales de la arquitectura presentada es la gran flexibilidad con la que cuenta, permitiendo la integración de sus componentes en más de una variante. Al igual que Rsyslog, Logstash permite la recepción de eventos directamente.

Por otro lado, Rsyslog implementa la posibilidad de enviar los eventos directamente hacia Elasticsearch, aunque no posee las posibilidades de filtrado y procesamiento de Logstash.

Un elemento fundamental a tener en cuenta en una arquitectura de gestión de trazas es la sincronización de tiempo. Debe estar configurado el servicio de tiempo en cada uno de los servidores mediante el protocolo NTP. Es esencial que funcione correctamente para que los datos de fecha y hora de las trazas sea consistente.

Conclusiones

En un sistema centralizado de gestión de trazas de seguridad es fundamental contar con mecanismos que posibiliten la generación de reportes y revisión periódica. Del análisis de las principales regulaciones y normas existentes se obtuvieron los componentes fundamentales y los eventos de mayor importancia a almacenar y analizar. La lista de registros de eventos propuestos puede variar en dependencia de las posibilidades tecnológicas en cuanto a recursos de hardware y software que se posean. Siempre se deben recolectar la mayor cantidad de trazas posibles si se tienen los medios para su almacenamiento seguro y revisión. La mayor información disponible debe provenir de los activos más críticos dentro de la red.

La propuesta del marco de trabajo descrito junto con la arquitectura centralizada va a proveer a los especialistas de seguridad y administradores de sistemas, la agrupación y síntesis de la información de seguridad generada. Provee de reportes y datos acelerando los tiempos de búsqueda, lo que puede contribuir positivamente a disminuir la brecha existente entre la ocurrencia de un ataque y la demora asociada a su descubrimiento.

Existen múltiples herramientas de software libre para la gestión de trazas, si es beneficiosa la diversidad existente, puede traer problemas a la hora de su selección he integración en un sistema centralizado. La arquitectura propuesta agrupa e integra los componentes de la gestión de trazas, tratando de usar el menor número de herramientas, en un sistema único donde se garantiza la recolección de los principales eventos de seguridad. Debido a su flexibilidad, la integración de las herramientas puede variar partiendo de los recursos y necesidades concretas del entorno donde se instale la solución.

Referencias

- ACCELOPS, 2013. Good Practice Guide (GPG13) Compliance in the UK. Successful Protective Monitoring with AccelOps. [en línea]. S.l.: [Consulta: 9 marzo 2015]. Disponible en: http://www.accelops.com/media/1697/AccelOpsGoodPracticeGuideSolutionBrief.pdf.
- BAKER, A.R., ESLER, J. y ALDER, R. 2007. Snort IDS and IPS toolkit. *Syngress, Canada*,
- BAKER, W., GOUDIE, M., HUTTON, A., HYLENDER, C.D., NIEMANTSVERDRIET, J., NOVAK, C., OSTERTAG, D., PORTER, C., ROSEN, M. y SARTIN, B. 2012. 2012 Data Breach Investigations Report. [en línea]. S.l.: [Consulta: 10 marzo 2013]. Disponible en: http://www.wired.com/images_blogs/threatlevel/2011/04/Verizon-2011-DBIR_04-13-11.pdf.
- BOTOND BOTYANSZKI 2009. NXLOG Community Edition Reference Manual for v2.8.1248 | nxlog.co. [en línea]. [Consulta: 21 enero 2015]. Disponible en: http://nxlog.org/documentation/nxlog-community-edition-reference-manual-v20928.
- BRAY, R., CID, D. y HAY, A. 2008. *OSSEC host-based intrusion detection guide*. S.l.: Syngress. ISBN 0080558771.
- CHUVAKIN, A., SCHMIDT, K. y PHILLIPS, C. 2012. *Logging and log management: the authoritative guide to understanding the concepts surrounding logging and log management*. S.l.: Newnes. ISBN 1597496367.
- COUNCIL, P.C.I. 2010. *PCI DSS 2.0*. S.l.: PCI Council Publication/United States.
- CSIS 2013. CSIS: 20 Critical Security Controls. [en línea]. [Consulta: 28 abril 2013]. Disponible en: http://www.sans.org/critical-security-controls/.
- FRY, C. y NYSTROM, M. 2009. *Security monitoring*. S.l.: O'Reilly Media, Inc. ISBN 0596555458.
- GORMLEY, C. y TONG, Z. 2014. *Elasticsearch: The Definitive Guide*. S.l.: O'Reilly & Associates. ISBN 1449358543.
- ISO, I. y STD, I.E.C. 2005. ISO 27002: 2005. *Information Technology-Security Techniques-Code of Practice for Information Security Management. ISO*,
- KENT, K. y SOUPPAYA, M.P. 2006. SP 800-92. *Guide to Computer Security Log Management, National Institute of Standards & Technology, Gaithersburg, MD*,
- KUĆ, R. y ROGOZIŃSKI, M. 2013. *Mastering ElasticSearch*. S.l.: Packt Publishing Ltd. ISBN 1783281448.
- MIC, 2007. *Resolución 127/2007 MIC. Reglamento de seguridad para las tecnologías de la información. Ministerio de la informática y las comunicaciones (MIC)*. 2007. S.l.: s.n.
- MICLEA, S. 2012. Windows and Linux Security Audit. *Journal of Applied Business Information Systems*, vol. 3, no. 4, pp. 117.

– NIST, S. 2007. 800-53. *Recommended Security Controls for Federal Information Systems*, pp. 800-53.
– RYBACZYK, P. 2005. *Expert Network Time Protocol: An Experience in Time with NTP*. S.l.: Apress. ISBN 1430200391.
– VERIZON 2014. 2014 Verizon Data Breach Investigations Report (DBIR) | Verizon Enterprise Solutions. [en línea]. [Consulta: 3 febrero 2015]. Disponible en: http://www.verizonenterprise.com/DBIR/2014/reports/rp_Verizon-DBIR-2014_en_xg.pdf.