Informe de Seguridad con Zabbix a empresa de servicios de entrega de productos que emplea el sistema SAP en la Cadena de Abastecimientos

Presentado por:

Alumno: MY. IVÁN D. FONSECA RODRÍGUEZ

Alumno: MY. DORLANDY A. PEÑA PARRALES

Alumno: MY. JOHN KEVIN NOYA DUARTE

Alumno: MY. RICHARD EDUARDO DURAN VILLANUEVA

Escuela Superior de Guerra ¨General Rafael Reyes Prieto¨

Curso de Estado Mayor – CEM 2025

Aula “Q”

Materia: Gestión de Riesgos Cibernéticos

Docente: Jaider Ospina Navas

19 de febrero de 2025, Bogotá D.C.

Introducción

En el entorno digital actual, la seguridad de los sistemas de información es un aspecto crítico para garantizar la integridad y continuidad operativa de las organizaciones. Por eso hoy en día las empresas deben ser conscientes de implementar los diferentes tipos de medidas preventivas, que garanticen identificar y clasificar las amenazas cibernéticas que podrían presentarse dentro de sus infraestructuras de plataformas informáticas, asegurando la continuidad del negocio y la confianza de sus clientes.

En la actualidad, una empresa de servicios de entrega de productos, líder en los procedimientos de logística de almacenamiento y entrega en la cadena de abastecimientos, que depende de su infraestructura tecnológica para gestionar sus operaciones a través del sistema SAP, acude a nuestra empresa, que emplea un sistema de planificación de recursos empresariales (ERP), y que a través de la plataforma de monitoreo de infraestructura Zabbix, se integra con este tipo de sistemas, para verificar las vulnerabilidades que pueden ser explotadas por ciberatacantes.

Este informe tiene como objetivo analizar los riesgos cibernéticos en la interconexión entre SAP y Zabbix utilizando un enfoque integral que combina los modelos STRIDE, PASTA y DREA, y propone la definición de controles de seguridad alineados con la norma ISO/IEC 27001: 2022 para mitigar las amenazas identificadas, garantizando la protección de la información.

Informe de Seguridad con Zabbix a empresa de servicios de entrega de productos que emplea el sistema SAP en la cadena de abastecimientos

1. Definición del Escenario

Como empresa contamos con un excelente sistema de monitoreo, para que sea utilizado por las **empresas de servicios de entrega de productos,** basados en la verificación de vulnerabilidades bajo el modelo de **Zabbix**; una plataforma de código abierto que permite la supervisión de la infraestructura de TI, incluyendo servidores, redes y dispositivos interconectados. Dado que **SAP** es el sistema central para la logística de la empresa, realizando el método de integración con Zabbix, para presentar vulnerabilidades que requieren mitigación.

Componentes Claves:

- **Zabbix**: Servidor central, agentes en servidores críticos, base de datos y frontend web.
- **Infraestructura**: Servidores para almacenamiento y procesamiento de datos, redes de interconexión con proveedores y clientes, dispositivos de monitoreo.
- **Usuarios**: Administradores de TI y empleados con permisos limitados según su función.

2. Descripción del Escenario

Infraestructura Tecnológica de Empresa de servicios de entrega de producto

- **SAP**: Utilizado para la gestión logística, en la Cadena de Abastecimientos
- **Zabbix**: Implementado como sistema de monitoreo de servidores, redes y aplicaciones.
- **Componentes clave**:
    - **Servidor central**: Procesa la información de SAP y envía alertas de seguridad.
    - **Agentes de Zabbix**: Instalados en servidores y dispositivos de la red.
    - **Base de datos**: Almacena logs, configuraciones y eventos de monitoreo.
    - **Usuarios**: Administradores de TI y personal con accesos limitados.

La integración de SAP con Zabbix permite una supervisión proactiva, pero también introduce vulnerabilidades críticas que deben ser gestionadas.

3. Análisis de Riesgos:

Se aplicaron los modelos STRIDE, PASTA y DREAD para identificar amenazas en SAP:

A. Analisis de amenaza con modelo STRIDE

Para evaluar las amenazas, se aplicó el modelo **STRIDE**, identificando las siguientes vulnerabilidades:

1. **Spoofing (Suplantación de identidad)**:

- **Amenaza**: Uso de credenciales robadas para acceder a SAP mediante vulnerabilidades.
- **Ejemplo de vulnerabilidad**: Escalada de privilegios en SAMR/LSAD mediante degradación de protocolo ("Badlock") (CVE-2016-0128 y CVE-2016-2118) (*cvss-v31-examples_r1*, s/f).

- **Mitigación**: Implementación de autenticación multifactor (MFA) y control de acceso basado en roles (RBAC).

2. **Tampering (Manipulación de datos)**:

- **Amenaza**: Modificación de registros en SAP no autorizados.
- **Ejemplo de vulnerabilidad en CVSS 3.1**: Inyección SQL almacenada en MySQL (CVE-2013-0375) (*cvss-v31-examples_r1*, s/f).
- **Mitigación**: Uso de consultas SQL parametrizadas y monitoreo de logs en tiempo real.

3. **Repudiation (Negación de responsabilidad)**:

- **Amenaza**: Eliminación de registros de auditoría en SAP desde una cuenta comprometida en Zabbix.
- **Ejemplo de vulnerabilidad en CVSS 3.1**: Corrupción de memoria en el motor de secuencias de comandos (CVE-2019-0884)
- **Mitigación**: Implementación de registros inmutables con Blockchain.

4. **Information Disclosure (Divulgación de información)**:

- **Amenaza**: Robo de credenciales mediante ataques Man-in-the-Middle en conexiones entre Zabbix y SAP.
- **Ejemplo de vulnerabilidad en CVSS 3.1**: Vulnerabilidad POODLE en SSLv3 (CVE-2014-3566) (*cvss-v31-examples_r1*, s/f)
- **Mitigación**: Uso exclusivo de **TLS 1.3** para cifrado de comunicaciones.

5. **Denial of Service (Denegación de servicio)**: Ataques DDoS contra servidores de monitoreo.

- **Amenaza**: Ataques DDoS dirigidos a los servidores de Zabbix para desactivar el monitoreo.
- **Ejemplo de vulnerabilidad en CVSS 3.1**: Denegación de servicio en Apple iWork (CVE-2015-1098) (*cvss-v31-examples_r1*, s/f).
- **Mitigación**: Implementación de sistemas de prevención de intrusiones (IDS/IPS) y balanceo de carga.

6. **Elevation of Privilege (Escalamiento de privilegios)**:

- **Amenaza**: acceso indebido a cuentas administrativas logrando ingreso root y comprometiendo SAP.
- **Ejemplo de vulnerabilidad en CVSS 3.1**: Vulnerabilidad en Cisco IOS que permite ejecución de comandos con privilegios administrativos elevados (CSCtr91106) (*cvss-v31-examples_r1*, s/f).
- **Mitigación**: Implementar segmentación de red y revisión continua de permisos.(*Software Secured | Comparison of STRIDE, DREAD & PASTA | USA*, s/f)

B. Aplicación del Modelo PASTA en el Monitoreo de SAP

El modelo **PASTA (Process for Attack Simulation and Threat Analysis)** permite dividir el análisis en diferentes fases del ciclo de vida de la información, abordando la seguridad desde una **perspectiva estructural**:

Fase PASTA	Aplicación en la Empresa usando (SAP)
Planning (Planificación)	Identificar la arquitectura de SAP y su monitoreo en Zabbix. Documentar riesgos asociados.
Access (Acceso)	Evaluar autenticación y control de acceso en SAP y Zabbix (MFA, RBAC).
Storage (Almacenamiento)	Revisar seguridad en bases de datos de SAP y registros en Zabbix.
Transmission (Transmisión)	Analizar cifrado de comunicaciones y riesgos de interceptación.
Application (Aplicación)	Evaluar vulnerabilidades en integraciones de SAP y Zabbix.

Ejemplo de Amenaza Analizada con PASTA: Vulnerabilidad CVE-2014-3566 (POODLE - SSLv3)

- **Fase PASTA Afectada**: Transmission (Transmisión)
- **Impacto en la Empresa**: Un atacante podría interceptar tráfico entre Zabbix y SAP si la comunicación no está protegida.
- **Mitigación**: Implementar TLS 1.3 y eliminar compatibilidad con versiones antiguas de SSL.(*Common Vulnerability Scoring System SIG*, s/f)

C. Evaluación de Riesgo con DREAD

El modelo **DREAD** nos ayuda a cuantificar el riesgo de cada vulnerabilidad identificada con **STRIDE y PASTA** mediante cinco factores:

Amenaza	D (Daño)	R (Reproducibilidad)	E (Explotabilidad)	A (Usuarios Afectados)	D (Detectabilidad)	Puntaje Total
Escalada de privilegios en SAP	9	8	7	9	5	**38 (Crítica)**
Inyección SQL	7	9	8	7	6	**37 (Alta)**
Denegación de servicio DDoS	6	7	9	8	5	**35 (Alta)**
Robo de credenciales (MITM - POODLE)	8	6	7	8	7	**36 (Alta)**

Ejemplo de Priorización con DREAD: Amenaza: Escalada de privilegios en SAP

- Puntaje DREAD: 38 (Crítica)
- Impacto: Acceso completo a la base de datos de la Empresa.
- Acción: Implementar MFA y RBAC, restringir acceso a cuentas privilegiadas.

D. Identificación de Amenazas Específicas

Componente	Posibles amenazas
Zabbix	Inyección SQL, escalamiento de privilegios, acceso indebido a logs.
SAP	Ataques de phishing, vulnerabilidades en API, ransomware.
Infraestructura	Ataques DDoS dirigidos, acceso físico no autorizado.

E. Priorización de Amenazas según su Impacto

Amenaza	Probabilidad	Impacto	Prioridad
Escalada de privilegios en SAP	Alta	Alta	Crítica
Inyección SQL en Zabbix	Media	Alta	Alta
Denegación de servicio	Alta	Media	Alta
Robo de credenciales por ataque MITM	Media	Alta	Alta

Finalmente, se logra identificar a través de **DREAD** que permitió cuantificar el riesgo de cada amenaza, priorizando la mitigación de aquellas con impacto crítico, como la escalada de privilegios y el acceso indebido a SAP.(Jain, 2021)

F. Matriz DAFO aplicada a la Seguridad del sistema SAP

El análisis de amenazas también debe complementarse con el contexto organizacional. La matriz DAFO proporciona una visión estratégica sobre los riesgos y oportunidades en la infraestructura tecnológica de la Empresa.

Debilidades	Fortalezas
Falta de conciencia en ciberseguridad	Políticas de seguridad bien definidas
Inseguridad en redes de comunicación	Uso de herramientas de seguridad avanzadas
Falta de un plan de recuperación ante incidentes	Respaldo y protección de datos
Ausencia de un plan de recuperación	Redundancia en sistemas críticos.
Software y sistemas desactualizados.	
Amenazas	**Oportunidades**
Incremento de ataques dirigidos	Implementación de nuevas tecnologías de seguridad
Vulnerabilidades en proveedores y terceros	Crecimiento en formación y capacitación en ciberseguridad.
Ingeniería social y suplantación de identidad	Aumento de alianzas estratégicas en Ciberseguridad
Amenazas persistentes avanzadas (APT).	Auditorías de seguridad en SAP
Amenazas internas no intencionadas	

G. Integración con Matriz DAFO

El análisis de amenazas debe complementarse con el contexto organizacional y de infraestructura. Al combinar DAFO con STRIDE-PASTA-DREAD, se pueden identificar soluciones estratégicas y operativas**.**(*Software Secured* | *Comparison of STRIDE, DREAD & PASTA* | *USA*, s/f)

Debilidad/Amenaza	Medida de mitigación (PASTA)	Priorización (DREAD)
Inseguridad en redes (D2)	Implementar TLS 1.3 y VPNs	Alta
Ingeniería social (A3)	Capacitación en seguridad, simulacros de phishing	Alta
Vulnerabilidades en terceros (A2)	Auditorías de seguridad a proveedores de SAP	Media

4. Diseño de Controles de Seguridad

Con base en el análisis de riesgos, se proponen las siguientes medidas de mitigación, de acuerdo al Anexo A (normativo) – Referencia de controles de seguridad de la información – ISO/CEI 27001:2022 (*ISO IEC 27001-2022.Español*, s/f), así:

Nº	TIPO DE CONTROL	CONTROL	MÉTODO
1	**Controles Tecnológicos**		
1.1.	Derechos de acceso privilegiado	La asignación y uso de los derechos de acceso privilegiado se restringirá y gestionará.	Restricción de accesos basada en roles (RBAC) para usuarios con privilegios elevados.
1.2	Autenticación segura	Las tecnologías y procedimientos de autenticación segura se implementarán en función de las restricciones de acceso a la información y la política específica del tema sobre el control de acceso.	Autenticación multifactor (MFA) para accesos críticos en Zabbix y en SAP.
1.3	Codificación segura	Los principios de codificación segura se aplicarán al desarrollo de software.	Implementación de TLS 1.3 para cifrado de comunicaciones
1.4	Protección contra malware	La protección contra el malware se implementará y respaldará mediante la conciencia adecuada del usuario.	Sistemas de detección de intrusiones firewall y (IDS/IPS) para prevenir ataques y accesos indebidos.
1.5	Protección de los sistemas de información durante las pruebas de auditoría	Las pruebas de auditoría y otras actividades de aseguramiento que involucren la evaluación de los sistemas operativos deben planificarse y acordarse entre el evaluador y la gerencia correspondiente.	Auditorías periódicas de vulnerabilidades en SAP y Zabbix.
1.6	Restricción de acceso a la información	El acceso a la información y otros activos asociados se restringirá de acuerdo con la política específica del tema establecida sobre el control de acceso.	Restricción de acceso a centros de datos con autenticación biométrica

2.	**Controles de Personas**		
2.1	Concientización, educación y capacitación en seguridad de la información	El personal de la organización y las partes interesadas relevantes deben recibir la conciencia, educación y capacitación adecuadas en seguridad de la información y actualizaciones periódicas de la política de seguridad de la información de la organización, las políticas y los procedimientos específicos del tema, según sea relevante para su función laboral.	Capacitación en ciberseguridad para reducir el riesgo de ataques de phishing y suplantación de identidad.
3.	**Controles Organizacionales**		
3.1	Políticas de seguridad de la información	La política de seguridad de la información y las políticas específicas del tema deben ser definidas, aprobadas por la gerencia, publicadas, comunicadas y reconocidas por el personal relevante y las partes interesadas relevantes, y revisadas a intervalos planificados y si ocurren cambios significativos.	Políticas de seguridad Zero Trust, para restringir accesos dentro de la red corporativa

Evaluación de las Medidas de Mitigación

Medida	Efectividad	Impacto en seguridad	Costo
MFA y RBAC	Alta	Alta	Bajo
TLS 1.3 y cifrado AES-256	Alta	Alta	Medio
IDS/IPS	Alta	Media	Alto
Auditoria Vulnerabilidades	Media	Alta	Alto

Conclusión y recomendaciones

El análisis de seguridad en la integración, a una empresa de servicios de entrega de productos que emplea el sistema SAP, bajo el seguimiento y monitoreo con la modalidad Zabbix en la cadena de abastecimientos, revela vulnerabilidades que podrían comprometer la continuidad operativa de la empresa, evidenciando que se detecta como las más críticas: el **escalamiento de privilegios, inyección SQL, ataques DDoS y robo de credenciales**. La combinación de los modelos **STRIDE, PASTA y DREAD** permitió no solo identificar amenazas, sino también priorizar su mitigación de manera efectiva.

Las principales recomendaciones incluyen:

1. **Implementar MFA y RBAC** para proteger accesos críticos en SAP.
2. **Actualizar protocolos de seguridad** eliminando SSLv3 y habilitando TLS 1.3.
3. **Fortalecer la detección de amenazas** con IDS/IPS y auditorías constantes.
4. **Capacitar al personal en ciberseguridad** para reducir ataques de ingeniería social.
5. **Efectuar auditorías periódicas** de vulnerabilidades en SAP.

Con estas medidas, empresa de servicios de entrega de productos que emplea el sistema SAP podrá reducir el riesgo de ciberataques, asegurando la protección de su infraestructura y la continuidad de sus operaciones logísticas en la Cadena de Abastecimientos.

Referencias

Common Vulnerability Scoring System SIG. (s/f). FIRST — Forum of Incident Response and Security Teams. Recuperado el 18 de febrero de 2025, de https://www.first.org/cvss/

Cvss-v31-examples_r1. (s/f).

ISO IEC 27001-2022.Español. (s/f).

Jain, S. (2021, abril 22). Threat Modelling Frameworks (SDL, STRIDE, DREAD & PASTA). *Medium*. https://radiumhacker.medium.com/threat-modelling-frameworks-sdl-stride-dread-pasta-93f8ca49504e

Software Secured | Comparison of STRIDE, DREAD & PASTA | USA. (s/f). Recuperado el 18 de febrero de 2025, de https://www.softwaresecured.com/post/comparison-of-stride-dread-pasta