Escuela Superior de Guerra “General Rafael Reyes”

Maestría en Ciberseguridad y Ciberdefensa

Gestión de Riesgos Cibernéticos

Aula R

Caso de Estudio

Estudio de Caso: Modelamiento de Amenazas Cibernéticas con STRIDE y Zabbix

Alumnos:

CC Diego Edison Cabuya Padilla

MY Sergio Cruz Baudín

MY Víctor López Salguero

CC Yerson Torres Bueno

Docente:

Jaider Ospina Navas

2025

Contenido

Tabla de figuras

Estudio de Caso: Modelamiento de Amenazas Cibernéticas con STRIDE y Zabbix

Introducción

Teniendo en cuenta la matriz DAFO desarrollada para el caso de estudio de la empresa Compumundohipermegared, se pudo identificar que el grado de exposición de la infraestructura tecnológica de la empresa no estaba documentado, lo que hace vulnerable no solo el modelo de negocio de la empresa sino la información de clientes y proveedores. Por tal razón se hace necesario realizar un estudio completo de la infraestructura de la empresa, así como establecer posibles vulnerabilidades a esta infraestructura para plantear controles y las modificaciones necesarias a la infraestructura.

1. Descripción del escenario

Compumundohipermegared es una empresa que proporciona servicios de internet, telefonía y televisión por cable, la empresa cuenta con una base de clientes de 100.000, con un crecimiento acelerado los últimos 2 años, que llevo a la empresa a efectuar un crecimiento en su infraestructura tecnológica y en la actualidad está visualizando crecer en su capital humano. El Equipo de TI de la empresa propuso incorporar una capa de seguridad a la infraestructura aprovechando la actualización por crecimiento, en junta directiva se aprobó el uso de Zabbix que es una herramienta de código abierto, para el monitoreo de infraestructura TI, permitiendo construir elementos y triggers personalizados para efectuar diferentes estilos de monitoreo de acuerdo a la necesidad de la empresa, esta herramienta también permite una gama de opciones para alertas personalizadas, visualización de datos , monitoreo distribuido, gestión de usuarios, personalización de informes, entre otras opciones (Lambert , et al., 2022).

De acuerdo con Aguilar se han presentado un aumento en brechas de información en el sector financiero, los ciberataques son cada vez más frecuentes, incidentes cibernéticos con connotaciones políticas y algunas impulsadas por grupos activistas y finalmente el hecho que acá en Latinoamérica 4 de cada 10 organizaciones sufrieron un incidente cibernético entre 2018 y 2019 (2020). Siendo este un panorama importante para tener en cuenta e implementar lo necesario para identificar vulnerabilidades y amenazas cibernéticas, con la finalidad de implementar y robustecer los controles de seguridad, para tal fin se tendrá como guía el modelo de amenazas STRIDE y el anexo A de la norma ISO 27001:2022.

2. Diagrama de la arquitectura de red de la empresa

La empresa cuenta con un servidor de base de datos, donde se almacena toda la información de usuarios, contabilidad y proveedores, se tiene un servidor de *backup* para esta información, un servidor central que maneja toda la parte de la seguridad de la empresa y donde se instaló Zabiix, un servidor que aloja el *frontend* web de la empresa.

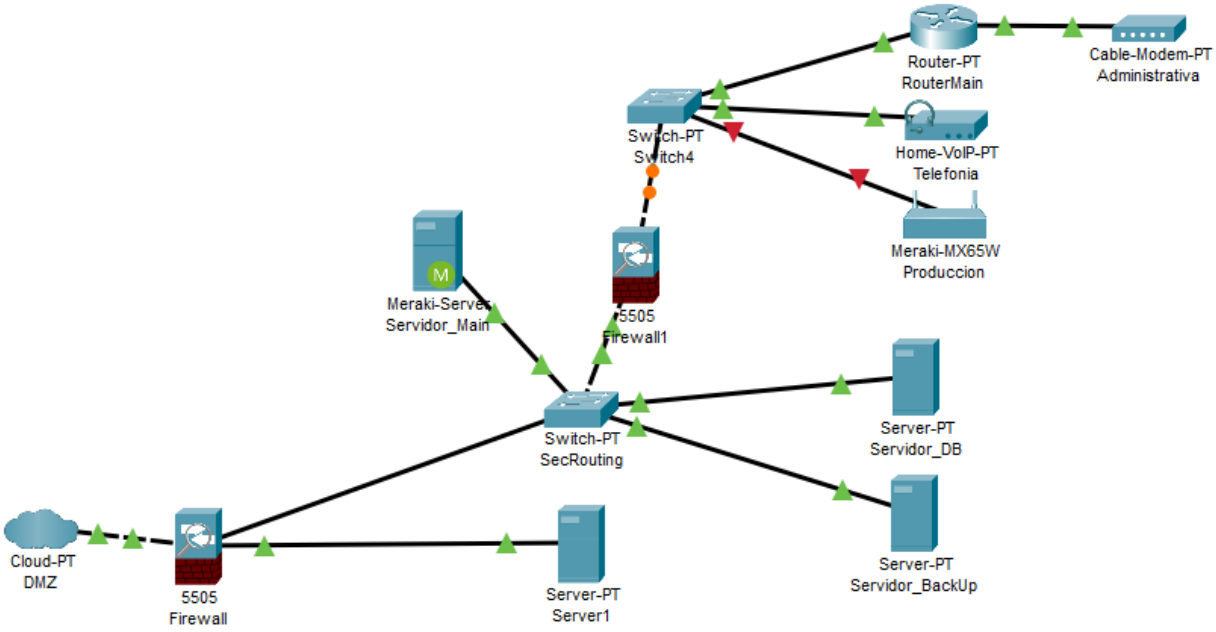

Figura 1. Arquitectura de red principal

Fuente: Elaboración propia

3. Análisis de riesgos y amenazas

Teniendo en cuenta el modelo STRIDE se pueden identificar amenazas que afectan la integridad, disponibilidad y confidencialidad de la información de la empresa, en estas categorías:

3.1. *Spoofing* (Suplantación de identidad)

Un atacante podría suplantar la identidad de un administrador o de un agente de Zabbix para acceder a la información sensible del sistema o realizar acciones no autorizadas, de acuerdo con el CVE-2022-23131, un atacante puede eludir la autenticación del sistema atacando directamente el *frontend* de Zabbix configurado con SAML, esta vulnerabilidad tiene una severidad de 9.1 (Haworth, 2022).

Componente afectado: Servidor central, agentes Zabbix.

3.2. *Tampering* (Manipulación de datos)

Un atacante podría tener acceso al sistema con el fin de modificar las configuraciones del servidor central, inyectar código malicioso en el *frontend* web o alterar datos almacenados en el servidor de base de datos, de acuerdo con el CVE-2024-42327 se puede inyectar arbitrariamente una instrucción de SQL, con un usuario sin ningún rol dentro del sistema y modificar datos de configuración o almacenados en el sistema, con roles privilegiados, esta vulnerabilidad tiene una severidad de 9.9 (Arghire, 2024).

Componente afectado: Servidor central, servidor de base de datos, *frontend* web.

3.3. *Repudiation* (Repudio)

Un atacante o usuario legitimo del sistema puede llegar a realizar alguna acción en la infraestructura y luego negar la realización de dichas acciones, lo que podría llegar a cambiar la configuración de Zabbix, borrar o corromper datos del sistema y no tener certeza de quien realizo la acción, de acuerdo con el CVE-2024-364660 permite acceder a las contraseñas de usuario de Zabbix, que daría fácil acceso y modificación de la configuración del sistema y a los logs, impidiendo que se tenga trazabilidad de los eventos efectuados, esta vulnerabilidad tiene una severidad de 8.1 (SOC team OGMA, 2024).

Componente afectado: Servidor central, servidor de base de datos.

3.4. *Information disclosure* (Divulgación de información)

Un atacante podría llegar a tener acceso a información sensible o confidencial del sistema Zabbix o del servidor de la base de datos, de acuerdo con el CVE-2024-36466 puede permitir a un atacante autenticarse en una sesión como administrador dándole acceso completo a la información del sistema, esta vulnerabilidad tiene una severidad de 8.8 (Arghire, 2024).

Componente afectado: Servidor central, servidor de base de datos.

3.5. *Denial of service DoS* (Denegación de servicio)

Un atacante podría intentar sobrecargar de solicitudes al servidor de Zabbix o al de base de datos, de igual forma podría llegar a interrumpir los equipos de red de la empresa, con peticiones de conexión fraudulentas, de acuerdo con el CVE-2024-36462 puede descontrolar el recurso de consumo de memoria del sistema, llevando a un atacante a generar un DoS de forma local en el sistema, esta vulnerabilidad tiene una severidad de 8.8 (Arghire, 2024).

Componente afectado: Servidores de la arquitectura o equipos de red.

3.6. *Elevation of privilege* (Elevación de privilegios)

Un usuario legitimo del sistema con acceso restringido, podría escalar sus privilegios para tener acceso a servidores, funciones o datos restringidos, de acuerdo con el CVE-2022-2313, un atacante puede eludir la autenticación del sistema atacando directamente el *frontend* de Zabbix y escalar de forma fácil sus privilegios como administrador, esta vulnerabilidad tiene una severidad de 9.1 (Haworth, 2022).

Componente afectado: Servidor central, servidor de base de datos.

La identificación de amenazas con el modelo STRIDE teniendo la arquitectura presentada en la Figura 1, donde se tiene el sistema Zabbix como orquestador de seguridad de la empresa, a pesar de que las amenazas tienen un fundamento técnico, es importante notar la importancia de tener una cultura en ciberseguridad, un paso importante como un control aplicado a toda la organización (personal y equipo) es estructurar una política de seguridad de la información que actúe como eje rector de la ciberseguridad en Compumundohipermegared (ISO, 2022).

4. Diseño de controles de seguridad

De acuerdo al diseño de la infraestructura de red de la empresa, *stakeholders* y empleados Compumundohipermegared y con las amenazas identificadas con el modelo STRIKE, siendo conscientes de las vulnerabilidades que actualmente tiene el sistema de la empresa, se proponen controles organizacionales, físicos y tecnológicos, con base en el anexo A de la Norma Técnica 27001:2022, dejando los controles de personas para una segunda fase de implementación cuando se gane madurez en el plan de capacitación de la política de seguridad de información y los acuerdos de servicio y confidencialidad firmado con los contratistas externos.

4.1. Controles organizacionales

Roles y responsabilidades de seguridad de la información (5.2)

Descripción: Definir los roles y responsabilidades de los *stakeholders* del sistema Zabbix, a partir del cargo o rol desempeñado en la empresa.

Control propuesto: Para este caso el equipo encargado en Compumundohipermegared se definirá a partir de este punto de la siguiente manera:

- Administrador de Zabbix (AZ): Encargado de configurar, operar y coordinar el mantenimiento del servidor Zabbix y sus agentes.

- Equipo de Seguridad TI (ES): Grupo de personas que se encarga de identificar, mitigar y monitorear amenazas de ciberseguridad, con ayuda del sistema Zabbix, firewall y alertas de los switchs.
- Administrador de Base de Datos (ABD): Encargado de gestionar el servidor de base de datos y el servidor de respaldo.
- Equipo de Red (ER): Grupo de personas que se encarga de administrar la infraestructura de red y dispositivos relacionados.
- Gerente de TI (GTI): Encargado de tomar decisiones estratégicas dentro de la arquitectura de red del sistema, de igual forma, rinde cuentas por la seguridad del sistema.
- Auditor de Seguridad (AS): Encargado de proporcionar revisiones independientes y asesoramiento sobre los diferentes riesgos del sistema.

  Esta organización orquestara las decisiones necesarias para que solo personal capacitado maneje el sistema, reduciendo riesgos de errores o accesos no autorizados.

Contacto con grupos de interés especial (5.6)

Descripción: Mantener contacto con foros especializados en seguridad, realizar vigilancia tecnología a sitios web como Security Week.

Control propuesto: Participar en grupos de la industria de telecomunicaciones, en especial en el foro de Zabbix (a través de la página https://www.zabbix.com/forum/zabbix-discussions-and-feedback), con la finalidad de verificar amenazas a sistemas de monitoreo, como vulnerabilidades en Zabbix y mantenerse actualizado con las mejores prácticas.

Seguridad de la información en la gestión de proyectos (5.8)

Descripción: Teniendo en cuenta la proyección de la empre en expandir el mercado, se debe integrar seguridad en la gestión de proyectos.

Control propuesto: Dentro de la infraestructura actual, implementando actualizaciones de Zabbix, se debe integrarlo con nuevos sistemas, se debe evaluar riesgos de seguridad desde el inicio, como proteger comunicaciones entre agentes y servidor, y documentar medidas en el plan del proyecto, es importante buscar la automatización de procesos dentro de la gestión de proyectos.

Planificación y preparación de la gestión de incidentes de seguridad de la información (5.24)

Descripción: Planificar y preparar para gestionar incidentes de ciberseguridad.

Control propuesto: Diseñar un plan que incluya escenarios donde Zabbix detecte accesos no autorizados o sea comprometido, con los roles definidos dentro de la organización, generar tareas específicas a cada rol o cargo con el fin de tener un equipo de respuesta óptimo para enfrentar dichos incidentes, disminuyendo su impacto en la organización.

Protección de registros (5.33)

Descripción: Proteger registros contra pérdida o acceso no autorizado, teniendo en cuenta las múltiples amenazas que pueden explotar las vulnerabilidades del sistema.

Control propuesto: Los logs y reportes de Zabbix deben cifrarse, almacenarse en un segmento del servidor de forma segura y respaldarse de forma regular, en una locación diferente, de igual forma el acceso debe ser restringido y solo a personal autorizado.

4.2. Controles físicos

Perímetros físicos de seguridad (7.1)

Descripción: Dentro de la infraestructura ya establecida, los perímetros de seguridad se definirán y utilizarán para proteger las áreas que contienen información y otros activos asociados, como servidores de base de datos, *backup* y el servidor principal de Zabbix. sistema.

Control propuesto: Se debe definir áreas seguras donde se encuentre el servidor Zabbix y la infraestructura relacionada, como salas de servidores de base de datos. Estas áreas deben estar protegidas con barreras físicas, como puertas de seguridad, y acceso restringido a personal no autorizado, mediante autenticación.

Monitoreo de seguridad física (7.4)

Descripción: Las instalaciones deben ser monitoreados continuamente para el acceso físico a las instalaciones.

Control propuesto: Se deben instalar cámaras de seguridad, sistemas de alarma, controles de acceso para monitorear en tiempo real las áreas donde está el servidor Zabbix y servidores de base de datos. Estos sistemas deben ser revisados periódicamente, de igual forma deben contar con un log que permita verificar cualquier intento de acceso no autorizado y establecer un plan de respuesta para mitigar riesgos.

4.3. Controles tecnológicos

Dispositivos de punto final de usuario (8.1)

Descripción: Se protegerá la información almacenada, procesada o accesible a través de los dispositivos finales del usuario.

Control propuesto: Los *endpoints* y agentes que acceden a la interfaz web de Zabbix, como estaciones de trabajo y servidores, se deben protegerse con actualizaciones regulares del sistema operativo, software antivirus y políticas de seguridad fuertes, de forma que se disminuya la superficie de ataque desde estas terminales.

Derechos de acceso privilegiado (8.2)

Descripción: El acceso se realizará por perfiles, teniendo en cuenta la asignación y uso de los derechos de acceso privilegiado se restringirá y gestionará con el rol adecuado.

Control propuesto: El acceso administrativo a Zabbix, que permite configurar el sistema y gestionar usuarios, se realizara mediante el rol de administrador Zabbix, con los permisos necesarios para realizar únicamente actividades de administración y debe restringirse a personal autorizado únicamente, se deben programar revisiones trimestrales de permisos y registro de actividades para detectar uso indebido de este perfil.

Autenticación segura (8.5)

Descripción: Las tecnologías y procedimientos de autenticación segura a los sistemas o equipos de la arquitectura de la empresa, se implementarán en función de las restricciones de acceso a la información y la política específica asociada a cada perfil de usuario, la cual tendrá un control de acceso especifico.

Control propuesto: La interfaz web de Zabbix debe usar conexión cifrada por HTTPS para comunicaciones seguras de punto a punto, se debe crear una política de cambio de contraseña con un periodo no superior a 3 meses, capacitar a los usuarios en la creación de contraseñas seguras e implementar la autenticación de dos factores para usuarios administrativos, se puede tener en cuenta que Zabbix en su versión 7.0 y posterior soportan múltiple factor de autenticación.

Conclusiones y recomendaciones

Al igual que para la empresa Compumundohipermegared, es primordial para cualquier organización, que maneje información digital, la identificación de vulnerabilidades de su infraestructura tecnológica, el grado de exposición de la misma y que hace vulnerable los

componentes de la empresa dentro del ambiente de producción, siempre teniendo presente que en la actualidad hay un aumento en brechas de información y ciberataques, lo que refuerza la necesidad de identificar vulnerabilidades y amenazas cibernéticas.

El Modelo STRIDE es de gran apoyo para identificar amenazas que afectan la integridad, disponibilidad y confidencialidad de la información, viendo las amenazas desde 5 puntos de vistas específicos que afectan la seguridad de la información de la organización, junto con la identificación de las amenazas se pudo verificar cuales vulnerabilidades puede llegar a ser explotadas y afectar el sistema de la organización.

Finalmente se puede establecer un modelo de sistema de seguridad capaz de identificar y actuar frente a una amenaza, siempre y cuando existan controles de seguridad, completamente definidos y para esto se tiene una guía importante como lo es la norma ISO 27001:2022, que da una guía muy aproximada a la organización diseminando 4 elementos de importancia dentro de sus controles, atacando las posibles brechas de seguridad de forma integral.

Referencias

Aguilar Antonio, J. M. (2020). La brecha de ciberseguridad en América Latina rente al contexto global de ciberamenazas. *Revista de estudios de seguridad internacional*, *6*(2), 17-43.

Arghire, I. (2024, diciembre 2). *Critical Vulnerability Found in Zabbix Network Monitoring Tool*. SecurityWeek. https://www.securityweek.com/critical-vulnerability-found-in-zabbix-network-monitoring-tool/

Haworth, J. (2022, febrero 18). *Critical vulnerabilities in Zabbix Web Frontend allow authentication bypass, code execution on servers*. The Daily Swig | Cybersecurity News and Views. https://portswigger.net/daily-swig/critical-vulnerabilities-in-zabbix-web-frontend-allow-authentication-bypass-code-execution-on-servers

Lambert, Dmitr., Baekel, B. van., & Lambert, D. Natha. (2022). Zabbix 6 IT Infrastructure Monitoring Cookbook.

SOC team OGMA. (2024, octubre 8). *Mitigating CVE-2024-36460: Plaintext Password Exposure in Zabbix Front-End Audit Log*. Mitigating CVE-2024-36460: Plaintext Password Exposure in Zabbix Front-End Audit Log. http://ogma.in/mitigating-cve-2024-36460-plaintext-password-exposure-in-zabbix-front-end-audit-log

Anexo – Matriz RACI

Implicaciones en la gestión de riesgos

R (Responsable): Es el responsable de ejecutar las acciones necesarias para mitigar el riesgo.

A (Accountable): Es quien tiene la autoridad para rendir cuentas y apruebar las decisiones.

C (Consulted): Persona o grupo de personas encargados de dar asesoramiento experto en el proceso de identificación y mitigación de riesgos.

I (Informed): Persona o grupo de personas encargados de recibir información sobre el progreso o los resultados.

Roles y responsabilidades

Administrador de Zabbix (AZ): Configura, opera y mantiene el servidor Zabbix y sus agentes.

Equipo de Seguridad TI (ES): Identifica, mitiga y monitorea amenazas de ciberseguridad.

Administrador de Base de Datos (ABD): Gestiona el servidor de base de datos y el servidor de respaldo.

Equipo de Red (ER): Administra la infraestructura de red y dispositivos relacionados a la arquitectura de la empresa.

Gerente de TI (GTI): Toma decisiones estratégicas y rinde cuentas por la seguridad del sistema a la gerencia.

Auditor de Seguridad (AS): Proporciona revisiones independientes y asesoramiento sobre riesgos de seguridad de la información.

Amenaza	Componentes Afectados	Responsables					
		AZ	ES	ABD	ER	GTI	AS
Suplantación (Spoofing)	Servidor central, agentes Zabbix	R	A	C	I	I	C
Manipulación (Tampering)	Servidor central, DB, frontend web	R	A	R	I	I	C
Repudio (Repudiation)	Servidor central, servidor de DB	R	A	R	I	I	C

Divulgación (Information Disclosure)	Servidor central, servidor de DB	R	A	R	I	I	C
Denegación (DoS)	Servidor central, DB, dispositivos de red	R	A	R	R	I	C
Elevación (Elevation)	Servidor central, servidor de DB	R	A	R	I	I	C

Suplantación de identidad (Spoofing)

AZ (R): Configura el sistema de autenticación en el servidor y agentes Zabbix.

ES (A): Define políticas de autenticación y supervisa el cumplimiento de estas.

ABD (C): Asegura que las credenciales (usuario y contraseña) en la base de datos estén protegidas.

ER (I): Informa sobre accesos sospechosos en la red.

GTI (I): Notifica del estado de las medidas implementadas.

AS (C): Asesora sobre mejores prácticas de autenticación.

Manipulación de datos (Tampering)

AZ (R): Implementa controles de integridad en el servidor y frontend.

ES (A): Valida medidas contra ataques como inyecciones SQL.

ABD (R): Protege la base de datos y el respaldo contra modificaciones no autorizadas.

ER (I): Informa acerca del monitoreo de tráfico anómalo.

GTI (I): Notificado el progreso.

AS (C): Proporciona asesoramiento e información sobre vulnerabilidades conocidas.

Repudio (Repudiation)

AZ (R): Configura logs de auditoría en Zabbix.

ES (A): Establece requisitos claros de auditoría y verifica su cumplimiento.

ABD (R): Garantiza la integridad de los logs de eventos en el servidor principal.

ER (I): Informa sobre incidentes relacionados con repudio.

GTI (I): Notificado de resultados.

AS (C): Asesora sobre estándares y correcto desarrollo de la auditoría.

Divulgación de información (Information Disclosure)

AZ (R): Implementa cifrado y controles de acceso en la arquitectura del sistema.

ES (A): Supervisa medidas contra fuga de información sensible.

ABD (R): Cifra datos sensibles en la base de datos y garantiza el acceso solo a personal autorizado.

ER (I): Informa acerca de brechas detectadas en la red.

GTI (I): Notifica el estado de seguridad.

AS (C): Asesora sobre protección de datos sensibles.

Denegación de servicio (Denial of Service)

AZ (R): Configura límites de recursos en el servidor Zabbix.

ES (A): Diseña estrategias contra ataques DoS.

ABD (R): Optimiza la base de datos para resistir sobrecargas y realiza el parcheo del sistema.

ER (R): Implementa filtros de red para mitigar ataques DoS.

GTI (I): Informado del impacto y medidas tomadas.

AS (C): Asesora sobre mitigación conocida de vulnerabilidades específicas.

Elevación de privilegios (Elevation of Privilege)

AZ (R): Asegura configuraciones de privilegios mínimos en Zabbix y segrega perfiles.

ES (A): Define políticas de acceso y verifica su implementación por roles.

ABD (R): Restringe privilegios en la base de datos a solo perfiles autorizados.

ER (I): Informa sobre intentos de escalamiento de privilegios detectados.

GTI (I): Notifica de resultados.

AS (C): Asesora sobre vulnerabilidades de escalamiento de privilegios.