¿Como Influyen los ataques de Ransomware en la infraestructura tecnológica de las empresas?

Juan Manuel Hurtado Lopez

Asesor

Alexander Larrahondo Nuez

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en Seguridad Informática

2025

Dedicatoria

Dedico mi tesis principalmente a Dios, por darme la fuerza necesaria para culminar esta meta. A mis padres, por todo su amor y por motivarme a seguir hacia adelante.

También a mis hermanos, por brindarme su apoyo moral en esas noches que tocaba investigar. Y, finalmente, a los que no creyeron en mí, con su actitud lograron que tomará más impulso.

Resumen

Actualmente los ataques de ransomware son los más comunes, esto debido a que algunas empresas no tienen la suficiente capacidad para mejorar su seguridad informática, lo que permite a los atacantes tener blancos fáciles, este ciberataque es frecuente debido que tiene como objetivo secuestrar datos y solicitar dinero a cambio de devolverlos, lo que trae beneficios lucrativos importantes para el delincuente.

De acuerdo con la empresa GREENCSS en el 2023, solo el 25% de las organizaciones en Latinoamérica no fueron atacadas por ransomware. El 49% sufrió entre uno y tres ataques, y el 26% fue atacada cuatro o más veces, estos datos reflejan la necesidad critica de que las empresas aumenten las estrategias efectivas de prevención y recuperación.

Palabras clave: Ataques, Ransomware, Ciberseguridad, Seguridad de la información, infraestructura.

Abstract

Ransomware attacks are currently the most common, due to the lack of sufficient capacity to improve their IT security, which allows attackers to have easy targets. This cyberattack is frequent because it aims to hijack data and demand money in exchange for its return, which brings significant lucrative benefits to the criminal.

According to GREENCSS, in 2023, only 25% of organizations in Latin America were not attacked by ransomware. Forty-nine percent suffered between one and three attacks, and 26% were attacked four or more times. These data reflect the critical need for companies to increase effective prevention and recovery strategies.

Keywords: infrastructure, Attacks, Ransomware, Cybersecurity, Information Security

Tabla de Contenido

Lista de Apéndices

Introducción

Actualmente los ataques de ransomware son los más comunes, esto debido a que algunas empresas no tienen la suficiente capacidad para mejorar su seguridad informática, lo que permite a los atacantes tener blancos fáciles y este método de ataque es frecuente debido que tiene como objetivo secuestrar datos y solicitar dinero a cambio de devolverlos, este tipo de amenazas es apetecida por los atacantes debido a que pueden tener beneficios lucrativos importantes.

Planteamiento del Problema

En los últimos años, el aumento de los ataques ransomware ha puesto en riesgo la infraestructura tecnológica de numerosas empresas a nivel global.

A pesar de las inversiones en seguridad informática, muchas organizaciones aun enfrentan dificultades para protegerse contra estos ataques. El problema radica en determinar la influencia especifica de los ataques de ransomware en la infraestructura tecnológica empresarial, explorando como estas amenazas afectan la gestión de TI, la recuperación de la información y la implementación de políticas de seguridad robustas.

En caso de que el riesgo de un ransomware se infiltre en la empresa, se tienen diez (10) impactos relevantes para la organización:

1) Perdida de datos: los atacantes tienen acceso a la información relevante permanente, incluso si se paga el rescate, ya que el ciberdelincuente puede quedar con copias de los datos.

2) Interrupción operativa: Se puede detener por completo las operaciones de la empresa, todo se puede paralizar hasta que sea resuelte la situación

3) Impacto financiero: Se unen varios factores que afectan la economía de la empresa en estas situaciones, además del costo del rescate, los costos adicionales por perdida de productividad, restauración del sistema, contratación de expertos en ciberseguridad y en algunos casos multas por incumplir normativas de protección de datos, son los factores que le pueden llegar a costar a la organización millones de dólares.

4) Daño reputacional: La pérdida de información genera desconfianza de los aliados estratégicos, por lo tanto, hay pérdida de clientes, inversiones.

5) Multas y consecuencias legales: La organización se puede ver expuesta a demandas y enfrentar situaciones legales por no custodiar los datos de manera adecuada.

6) Filtración de información confidencial: Las amenazas de los atacantes es filtrar la información y publicar los datos al público si no se paga el rescate.

7) Costos de recuperación: Restaurar el sistema puede tardar, se hace un proceso lento y es costoso para la organización, adicional de la contratación de expertos para tomar medidas de seguridad para evitar futuros ataques.

8) Pérdida de confianza interna: un ataque de este tipo puede llegar afectar a los empleados tomando desconfianza en los sistemas, bajando la productividad.

9) Aumento en la prima de seguros: como todo seguro, cada que se ve afectada la póliza de seguros, estas tienen un aumento para su renovación lo que genera dificulta para renovar o adquirir nuevos seguros.

10) Impacto en la infraestructura critica: Si la empresa se dedica a prestar servicios hospitalarios, energéticos, combustibles, o servicios que afecten directamente al usuario o haya riesgo de vidas de personas, las consecuencias pueden ser más graves.

De acuerdo con lo indicado por la compañía Kaspersky entre junio de 2023 y julio de 2024 hubo un aumento del 2,8% en ataques ransomware. En América Latina Hubo 1.185.242 ataques, es decir, 3 247 al día. Colombia ocupa el cuarto puesta dentro de la lista de países más atacados, lo que lleva a las organizaciones colombianas a aumentar su seguridad y así evitar consecuencias reputacionales, perdida de información, para de operaciones y principalmente pérdidas económicas significativas.

Justificación

Cada día aumentan las amenazas digitales, tanto en cantidad como en sofisticadas, es por esto por lo que la seguridad informática toma gran importancia porque aportan buenas prácticas para la gestión de los servicios de TI y su infraestructura.

Las organizaciones al implementar y tener bases solidad de seguridad informática pueden reducir o mitigar los riesgos cibernéticos de manera más eficiente, aumentando la agilidad en los tiempos de respuesta de incidentes de seguridad y siendo más eficiente en toda el área de TI ante la problemática que trae los avances tecnológicos.

Objetivos

Objetivo General

Analizar el impacto de los ataques de ransomware en la infraestructura tecnológica de las empresas del sector petrolero y energético en Colombia, determinando las principales vulnerabilidades, las consecuencias operativas, medidas preventivas y las estrategias de respuesta más efectivas para fortalecer la ciberseguridad empresarial

Objetivos Específicos

Conocer los ataques ransomware más relevantes que existen actualmente y como afectan a las empresas del sector petrolero y energético en Colombia, lo que permite identificar controles y métodos de seguridad como métodos de prevención de ataques ransomware.

Identificar como desde la seguridad informática se puede aportar para la solución de ataques ransomware en las empresas del sector petrolero y energético.

Investigar las medidas preventivas y políticas de ciberseguridad que las empresas del sector petrolero y energético adoptan para protegerse contra futuros ataques de ransomware.

Comparar las diferentes infraestructuras y estrategias de seguridad en las organizaciones petroleras y energéticas de Colombia, frente a los ataques ransomware, conociendo los métodos de prevención de ataques más comunes, económicos y eficientes que las empresas puedan adoptar.

Marco Referencial

Antecedentes

Para el desarrollo de este proyecto, se tomará como referencia el marco de ciberseguridad del NIST, el cual es creado por el instituto nacional de estándares y tecnologías de los estados unidos, el cual ayuda a los negocios de todo mundo y tamaño a comprender mejor sus riesgos de ciberseguridad, así como administrarlos y reducirlos.

Ofrece las mejores prácticas para que los negocios sepan donde centrarse y decidir dónde invertir el tiempo y dinero en cuestión de protección de ciberseguridad

(Comisión Federal del Comercio, 2024)

Marco Conceptual

El ransomware es un tipo de malware o virus que encripta los datos cuando se logra llegar a ellos, haciendo que la víctima no pueda llegar a ellos, tanto que el atacante exija un pago por ellos, por su rescate.

Existen varios tipos de ransomware entre los más importantes están cryto, locker, y Raas, los dos primeros son ataques de encriptar y cifrar la información para exigir un rescate y el ramnsomware Raas, es un tipo de servicio donde venden los códigos maliciosos para luego ser usados. Estos ataques son propagados por medio de phishing, exploit kits, correos electrónicos maliciosos y descargas involuntarias.

La infraestructura implementada en las empresas juega un papel muy importante, hoy en día las empresas utilizan marcos de referencia, certificaciones, referencias de seguridad que ayuden a robustecer la seguridad de la información, previniendo ataques y mitigando riesgos que generan

los ataques cibernéticos hoy en día. También como estrategia de ciberseguridad que ayuda a mantener la infraestructura segura es tener métodos para detectar huecos de seguridad, identificar vulnerabilidades, políticas de seguridad inadecuadas o insuficientes.

Es fundamental aprovechar las tecnologías que hoy en día ofrece el mercado, las empresas deben adoptar herramientas EDR (Endpoint Detection and Response), especiales en inteligencia de amenazas o soluciones basadas en inteligencia de artificial para detectar patrones de ransomware.

Cundo no se tiene una seguridad adecuada, y los ataques ransmware cumplen su objetivo, se presentan consecuencias significativas para las organizaciones como, por ejemplo, interrupción operativa, perdida de datos, costos financieros, reputación, que pueden llevar a las empresas hasta la quiebra.

Una de las consecuencias más graves para las empresas son las pérdidas económicas que se pueden presentar por un ataque ransomware. En el 2023 el rescate promedio ascendió a $1.54 millones de dólares, casi el doble del año anterior (Avella, 2023)

Como recomendación de las mejores prácticas de ciberseguridad para prevenir grandes consecuencias derivadas de los ataques ransomware es tener una buena gestión de copias de seguridad, para tener como recuperar la información en caso de perdida, tener un buen programa de concientización y sensibilización a los empleados, pues estos se consideran un eslabón débil en la cade de seguridad, adicional tener una buena estrategia de recuperación de desastres y respuesta a incidentes, de tal forma que las organizaciones se puedan levantar rápido de un ataque de este tipo.

Hay varias teorías o marcos que se pueden utilizar como la de resiliencia organizacional, teoría

de gestión de riesgo, que permita identificar, evaluar, y priorizar el riesgo llevándolo a la mitigación; existen muchas otras teorías y marcos que pueden ayudar a las organizaciones a tener una eficiente gestión de la ciberseguridad como lo relacionamos en el marco de referencia el marco de ciberseguridad NIST.

Resultados

Ataques Ransomware más Relevantes

Los ataques ransomware se conocen por grupos o se dividen en grupos, algunos de los más relevantes de los últimos años y que actualmente siguen causando daño son:

Darkside Ransomware

Fue utilizado en uno de los ataques más destructivos

realizado a la empresa de oleoductos estadunidense “Colonial Pipeline” en 202, utiliza un modelo RAAS, hace su primera aparición en agosto de 2020.

Maze Ransomware

Apareció en el 2019 y se distribuye a través de enlaces maliciosos, archivos adjuntos, ataques de fuerza bruta o kits de exploits, si la victima cae y no hay seguridad preventiva, el software se despliega y cifra los archivos.

Aunque indican que se había disuelto en 2020, hoy en día se han encontrado ataques que siguen el módulo operandi en las nuevas variedades de ransomware.

Lockbit Ransomware

Es de los ataques ransomware que más víctimas tuvo durante el primer trimestre de 2024, se han detectado nuevas versiones personalizadas de este programa.

DoppelPaymer ransomware

Fue considerado uno de los grupos ransomware más nocivos en 2023. Fue el tipo de ataque que afecto la petrolera mexicana Pemex. Este tipo de ransomware bloquea la información y manda notas de rescate indicando que tienen 7 días para pagar el rescate.

Nuevas Apariciones De Ataques Ransomware

- 8BASE, es uno de los que más víctimas tiene durante el 2024.

- AKIRA, Dirigido a sistemas Windows y Linux, también se encuentra en el top 10 de los ataques con más víctimas durante el 2024.
- PLAY: Se encuentra junto a 8base dentro del top 5 de familias de ransomware que tienen más víctimas en el primer trimestre del 2024, (S2GRUPO, 2024)

En Colombia los ataques ransomware como servicio (Raas) ha facilitado a los ciberdelincuentes lanzar ataques con mayor facilidad, los ransomware tipo Raas, ha ganado terreno, ya que hay grupos de delincuentes ofreciendo herramientas de ransomware a terceros, aumentando el número de ataques en el país.

Los ataques de ransomware en Colombia espáticamente al sector petrolero y energético han sido de alto impacto para este tipo de empresas. El caso más reciente es el ataque a la empresa Air-e empresa que genera energía a la costa atlántica en el país, causando retrasos en las operaciones y para los usuarios. El ataque logro vulnerar el SOC de claro Colombia y Kaspersky, de acuerdo con declaraciones de la empresa se procedió a restaurar los sistemas comprometidos, (MuchoHacker.LOL, Empresa Air-e sufre ataque de ransomware, 2024)

En el año 2022 la empresa EMP sufrió ataque tipo ransomware por el grupo BlackCat Alphv, donde se comprometieron datos sensibles de la organización, de acuerdo con las investigaciones, el ataque vino desde un adentro de la organización ya que se tuvo acceso a la data center alterno, (MuchoHacker.LOL, Grupo BlackCat Alphv publica pruebas de ataque ransomware a EPM, 2022).

Empresas como Ecopetrol, ISA, XM, son consideradas infraestructuras físicas y digitales criticas para la seguridad energética del país, estas empresas cuentan con seguridad informática de alta calidad como por ejemplo herramientas de seguridad o de alertamiento, SOC y cuentan con equipos humanos muy calificados, Además con empresas que cuentan con una alta

gobernabilidad e TI, donde se evalúan los procesos, los controles generados para cada riesgo.

Estas empresas pueden servir de ejemplo en seguridad o ciberseguridad ya que, a pesar de ser tan apetecidas por los ciberdelincuentes, aun no presentan ataques efectivos que afecten la seguridad de la organización.

Como desde la Seguridad Informática se Puede Aportar para la Solución de Ataques Ransomware en las Empresas del Sector Petrolero y Energético

Lo primero que se debe de aceptar por parte de las organizaciones y los usuarios que las componen es que la delincuencia se ha trasladado a un mundo digital cada vez más amplio, desde este punto de vista, las empresas deben de dar la importancia suficiente a la seguridad informática tanto que se debe adicionar o tener en el plan estratégico de la compañía.

Toda empresa en los procesos de TI, y teniendo en cuenta que las organizaciones del sector petrolero y energético son empresas grandes deben contemplar tener un área de ciberseguridad la cual contemple procesos, como gestión de riesgos, quipo de amenazas y monitoreo y equipos de Devsecops que se encargue de revisar los proyectos salientes.

Desde la seguridad informática, se puede tomar en cuenta la capacitación del personal, gran parte de los ataques van dirigidos a los empleados, tomándolos como el eslabón más débil de la seguridad, desde la seguridad informática se deben llevar a cabo capacitaciones, charlas que lleven los empleados a estar alertas, tener conocimientos suficientes para evitar un incidente de seguridad.

Medidas Preventivas y Políticas de Ciberseguridad que las Empresas el Sector Petrolero y Energético Adoptan para Protegerse

Las empresas del sector petrolero y energético por lo general son empresas grandes, tienen un buen gobierno corporativo y Gobernanza de TI, lo cual hace que sus políticas y

procedimientos sean evaluados constantemente ya sea por auditoría interna, auditorías externas, revisoría fiscal y permanezcan en constante evolución o mejora continua.

Además de tener herramientas y aplicaciones de buena calidad para la gestión de la seguridad como por ejemplo Crowdstrike, Lumo, Microsoft defender, antivirus de buena calidad, SOC, estas empresas cuentan con un área muy importante como lo es la gestión de riesgos de ciberseguridad, que se encarga de buscar riesgos de ciberseguridad y buscar la solución más adecuado para que los riesgos sean mitigados, así estas empresas aceleran el cierre de huecos de seguridad.

Comparar las Diferentes Infraestructuras y Estrategias de Seguridad en las Organizaciones Petroleras y Energéticas De Colombia, Frente a los Ataques Ransomware, Conociendo los Métodos de Prevención de Ataques más Comunes, Económicos y Eficientes Que las Empresas Puedan Adoptar

La infraestructura de estas empresas esta soportada en servicios de la Nube, las estrategias de seguridad se basan en tener segmentación de Red, copias de respaldo, herramientas de monitoreo, inteligencia de amenazas y antivirus que ayuden a prevenir los ataques.

No es mucha la diferencia que se presenta en las empresas, algunas tienen más herramientas que otras, sin embargo, las empresas de e3ste sector, gestionan la seguridad de la información de una forma muy similar, de tal forma que lo ataques no sean efectivos.

La prevención de ataque más comunes y económicas además de efectivas que puedan adoptar las empresas son:

- Capacitaciones como se indicó anteriormente, es intuir a los empleados para que tengan el conocimiento suficiente y se pueda prevenir ataques
- Generar copias de seguridad, si bien requiere presupuestó, hay varias formas de

gestionar copias de seguridad, es un control de gran importancia frente a los atauques ransomware. En caso efectivo de perdida de información se pueda

recuperar, para esto es muy importante adicional las pruebas de restauración, que garantice que las copias de seguridad se pueden restaurar sin problema.

- Tener un plan de aplicación de parches o actualizaciones de aplicaciones.
- Tener controles de gestión de accesos, políticas estrictas de contraseña y autenticación multifactor.

Los anteriores son métodos, políticas ´+, controles que las empresas pueden implementar, además de ser efectivas frente a ataques ransomware, son económicas y fácil de implementar.

Conclusiones

Las amenazas cibernéticas representan una problemática en el mundo digital actual. Desde el robo de datos personales hasta ataques contra infraestructura críticas. Estas problemáticas son un gran desafío para la seguridad de las organizaciones y personas. La seguridad informática es una prioridad hoy en día, esto implica capacitación de personas, herramientas de seguridad actualizadas, implementación de estrategias y marcos de TI eficientes. Adicional los especialistas en seguridad informática deben capacitarse y enfocar sus esfuerzos en aportar en la solución de las problemáticas actuales. Esto raíz del aumento significativo de ataques ransomware en Colombia, las organizaciones se deben implementar estrategias adecuadas para la protección de los activos de información, utilizar herramientas de alta tecnología y aprovechar la inteligencia artificial como gran aliado para soluciones tecnológicas e implementación defensa de la seguridad de la información.

Referencias Bibliográficas

Castro, M. M. (2022). La Respuesta a Incidentes en un Escenario Global y Con Protagonismo Del Ransomware . *Revista de Unidades de Información*.

Dustyn Zamora Baida, A. T. (09 de 12 de 2020). Análisis y técnicas de prevención ante ataques. *Revista tecnologica ciencia y educación*.

Fuentes, X. F. (2023). Técnicas de análisis forense para la evaluación de la privacidad e integridad de la información: navegadores web y ataques de ransomware. *Centro Singular de Investigación en Tecnologias de Intelixentes*.

hyperconectado. (2022). *Grupo BlackCat Alphv publica pruebas de ataque ransomware a EPM.* MuchoHacker.LOL.

Kasperky. (2020). Los principales ataques de ransomware. *Kasperky*.

Niño, F. Y. (28 de 06 de 2022). Ransomware, una amenaza latente en Latinoamérica. *ESP Sede del Pacifico*.

Reshmi, T. (2021). Information security breaches due to ransomware attacks - a systematic literature review. *International Journal of Information Management Data Insights*.

Romero Rubiano, J. E. (2023). Ciberataques: análisis de Ransomware y métodos de protección. *Universidad Oberta de Catalunya*.

Salinas Zambrano, Á. M. (2023). Guía de buenas prácticas para prevenir y reaccionar ante un ataque de ransomware. *PUCE - Ambato*.

Apéndices

Apéndice A

Glosario

Ataque Cibernético

Es cualquier esfuerzo intencional para robar, exponer, alterar, deshabilitar o destruir datos, aplicaciones u otros activos a través del acceso no autorizado a un red, sistema informático o dispositivo digital.

Ciberseguridad

Es la práctica de proteger equipos, redes, aplicaciones de software. sistemas críticos y datos de posibles amenazas digitales.

Infraestructura

Es un conjunto de instalaciones, servicios y medios técnicos que soportan el desarrollo de actividades.

Ransomware

En español secuestro de datos, es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema operativo.

Seguridad de la Información

Es un conjunto de procedimiento y herramientas de la seguridad que protegen ampliamente la información.