UNIVERSIDAD TECNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN FINANZAS E INFORMÁTICA

CARRERA DE SISTEMAS DE INFORMACIÓN

PROCESO DE TITULACION

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN SISTEMAS DE INFORMACIÓN

TEMA:

ANÁLISIS DE ESTRATEGIAS DE RECUPERACIÓN FRENTE AL IMPACTO DE LOS RANSOMWARE EN OFICINAS DE LA FACULTAD DE ADMINISTRACIÓN FINANZAS E INFORMÁTICA DE LA UNIVERSIDAD TÉCNICA DE BABAHOYO.

ESTUDIANTE:

JUAN CARLOS GARCÍA VEGA

TUTORA:

ING. NELLY ESPARZA CRUZ

AÑO

2024

CONTENIDO

INDICE

RESUMEN 3

PLANTEAMIENTO DEL PROBLEMA 5

JUSTIFICACIÓN 7

OBJETIVOS DEL ESTUDIO 9

LÍNEA DE INVESTIGACIÓN Y ARTICULACIÓN DEL TEMA 10

MARCO CONCEPTUAL 11

MARCO METODOLÓGICO 25

RESULTADOS 27

DISCUSIÓN DE RESULTADOS 29

CONCLUSIONES 31

RECOMENDACIONES 32

REFERENCIAS BIBLIOGRÁFICAS 33

ANEXOS 35

RESUMEN

Este caso de estudio se enfoca en las estrategias que se pueden aplicar ante la situación de presentarse una infección o ataque por ransomware y el impacto que este podría tener en las oficinas de la facultad de administración, finanzas e informática de la Universidad Técnica de Babahoyo.

Se hace referencia a un problema persistente, ya que actualmente en todos lados se enfrenta a constantes amenazas de virus específicamente hablando en el contexto de ataques ransomware; estos comprometen la seguridad de los equipos afectando a los archivos y a la confidencialidad de estos haciendo crítico el cuidado del activo más valioso que tiene la empresa que es la información.

El no tener un enfoque tecnológico de preparación y coordinado para hacerle frente a estas amenazas pueden dar lugar a consecuencias graves que podrían ser irreversibles ante el daño de los datos y la interrupción prolongada de las operaciones y servicios muy esenciales de la facultad lo que también sería un impacto negativo en la reputación de la institución.

En este trabajo se expone como objetivo analizar estrategias de recuperación relacionadas con la recuperación frente al impacto de los ransomware en oficinas de la facultad de administración finanzas e informática.

Además, cuenta con una metodología cualitativa que fortalece a la investigación ya que se ha elaborado una entrevista a un experto en tecnología y seguridad informática que describe ciertas pautas entorno a esta amenaza como son los ransomware.

Así mismo al final del estudio se puede encontrar con recomendaciones que pueden ser tomadas estratégicamente para aportar en la mitigación y prevención de estas amenazas.

PALABRAS CLAVES

Ransomware, TI, seguridad informática, firewall, ciberdelincuentes, spyware.

ABSTRAC

This case study focuses on the strategies that can be applied in the event of a ransomware infection or attack and the impact that this could have on the offices of the Faculty of Administration, Finance and IT of the Technical University of Babahoyo.

Reference is made to a persistent problem, since currently everywhere is faced with constant virus threats specifically speaking in the context of ransomware attacks; These compromise the security of the equipment, affecting the files and their confidentiality, making it critical to take care of the most valuable asset that the company has, which is the information.

Failure to have a prepared and coordinated technological approach to address these threats can lead to serious consequences that could be irreversible due to data damage and prolonged interruption of very essential operations and services of the faculty, which would also be a negative impact on the reputation of the institution.

The objective of this work is to analyze recovery strategies related to recovery from the impact of ransomware in offices of the Faculty of Administration, Finance and IT.

In addition, it has a qualitative methodology that strengthens the research since an interview has been carried out with a technology and computer security expert who describes certain guidelines regarding this threat such as ransomware.

Likewise, at the end of the study you can find recommendations that can be taken strategically to contribute to the mitigation and prevention of these threats.

KEYWORDS

Ransomware, IT, computer security, firewall, cybercriminals, spyware.

PLANTEAMIENTO DEL PROBLEMA

Actualmente en las oficinas de la facultad de administración, finanzas e informática de la Universidad Técnica de Babahoyo se enfrentan constantemente a amenazas de virus específicamente hablando en el contexto de ataques ransomware; estos ataques comprometen la seguridad de los equipos afectando a los archivos y a la confidencialidad de estos haciendo crítico el cuidado del activo más valioso que tiene la institución que es la información.

También se podría generar continuamente interrupciones significativas en las operaciones de la institución a pesar de los esfuerzos que se realizan o se implementen estos ransomware tienen una naturaleza sofisticada, pues evolucionan y mutan dejando así en una posición vulnerable la continuidad de las actividades académicas y administrativas en la facultad.

El ataque de ransomware podría generar una crisis grande y significativa en las oficinas de la facultad de administración, finanzas e informática haciendo un problema institucionalmente gigante pues es un incidente que puede comprometer la confidencialidad e integridad de datos académicos y estudiantiles que causaría retrasos e incidentes en las operaciones diarias generando preocupación en las autoridades y en el personal administrativo de la facultad, ya que la falta de acceso a la información primaria podría ocasionar incertidumbre sobre su recuperación resaltando estas vulnerabilidades como agujeros de seguridad cibernéticas en la facultad.. (FritzGerard, 2022)

Es un inconveniente complejo el ser atacado de ransomware, pues su recuperación establece metodologías complicadas y avanzadas en muchos casos con impactos graves donde la recuperación es nula y estas pueden ocasionar un impacto negativo grave en las oficinas de la facultad de administración, finanzas e informática, pues los ataques se caracterizan por tener un cifrado complejo de datos para su posterior extorsión comprometiendo de esta manera la continuidad del negocio y la integridad de información.

La creciente amenaza por la existencia de los ransomware ha conllevado a un aumento significativo de ciberataques dirigidas especialmente a empresas y sobre todo a instituciones educativas donde confluye bastante cantidad de personas y por ende tienen

manejo a muchos intercambios de archivos de forma descontrolada, estos ataques pueden incurrir en las oficinas de administración, finanzas e informática por lo que en este contexto el presente trabajo de caso de estudio se centra en realizar un análisis exhaustivo para construir estrategias técnicas de recuperación bien elaboradas que permitan reducir la incidencia de algún impacto negativo y devastador de los maliciosos ransomware.

Además, la presión para el encuentro de soluciones rápidas y eficientes que puedan ser efectivas es un desafío constante a considerar para el equipo de tecnologías de la información de la Universidad Técnica de Babahoyo y la parte administrativa planteando necesidades estratégicas de recuperación con medidas preventivas de algún futuro ataque.

El problema de este caso de estudio se centra en un esquema o política institucional que debe existir para contrarrestar y sobre todo tener una prevención ante ataques de ransomware, pues se evidencia que se carece de estrategias institucionales de recuperación para las oficinas de la facultad de administración, finanzas e informática y seguramente para el resto de oficinas también. El no tener estos enfoques tecnológicos coordinados para hacerle frente a estas amenazas pueden dar lugar a consecuencias graves que podrían ser irreversibles ante el daño de los datos y la interrupción prolongada de las operaciones y servicios muy esenciales de la facultad lo que también sería un impacto negativo en la reputación de la institución. (Mieles, 2021).

JUSTIFICACIÓN

Es importante analizar el impacto que tendría un ataque ransomware en la facultad de administración, finanzas e informática se justifica debido a la creciente amenaza que este tipo de virus destructivo representa para el entorno educativo y administrativo en este caso de estudio se demuestra una oportunidad interesante que permite comprender de forma holística las implicaciones académicas y operativas asociadas al índice de inseguridad cibernética que siempre está presente.

Analizar las estrategias de recuperación que se quieren implementar luego de algún ataque ransomware proporcionaría una visión o panorama crítico sobre la efectividad de las medidas que se puedan tomar para una mitigación eficiente. Además, explorar las dificultades con las que se podría encontrar por algún equipo del departamento de tecnologías de información permitiría una valiosa información a la comunidad informática sobre los desafíos operativos que se han logrado después de un ataque de ransomware.

Esta investigación de caso de estudio no solo servirá para comprender mejor la dinámica de funcionamiento de los ciberataques en el sector educativo, sino que además también permitirá desarrollar algunas recomendaciones concretas y prácticas para de esta forma fortalecer una postura de seguridad en la facultad ayudando de esta manera en la prevención y mitigación de futuros incidentes de ransomware.

Por lo que se considera que se requiere poner a consideración la protección de la información sensible, es decir que a las oficinas donde se manejan datos sensibles administrativos y académicos deben tener una cultura de cuidado para prevención, pues la pérdida o falta de compromiso en cuanto al cuidado de los datos puede acarrear consecuencias graves en lo que concierne a la confidencialidad y a la integridad de la información.

(Santana, 2022) Opina que, es necesario entender que realizar este caso de estudio permitiría la implementación eficaz de estrategias de recuperación necesarias para garantizar la continuidad de operaciones académicas y administrativas reduciendo el impacto que pueden causar las amenazas cibernéticas como los ransomware, garantizando de esta manera la continuidad de las operaciones.

Una respuesta efectiva no solo permitiría proteger la información, sino que también permitiría demostrar el grado de compromiso que la facultad tiene con la seguridad y la integridad de su información, fortaleciendo de esta manera la confianza de sus estudiantes, personal administrativo y otras partes interesadas de la facultad.

La naturaleza cambiante en relación a los ataques ransomware, requieren una adaptación constante de estrategias de recuperación establecidas como políticas. En tal sentido, este estudio de caso contribuirá en gran dimensión a la comprensión de tácticas actuales más efectivas, permitiendo que las oficinas de la facultad mantenerse con bajo riesgo ante amenazas emergentes (Barry Seal, 2021).

En este contexto, es necesario que se aborde la siguiente pregunta: ¿Cómo pueden las oficinas de la Facultad de administración, finanzas e informática mejorar sus estrategias de recuperación y de esta manera minimizar el impacto de los ataques de ransomware y lograr garantizar una continuidad en sus operaciones de manera eficiente y segura? La respuesta a esta interrogante, no solo tiene relación con la protección de la información, sino también en la preservación de su integridad y su reputación institucional.

OBJETIVOS DEL ESTUDIO

Objetivo General

Analizar estrategias de recuperación relacionadas con la recuperación frente al impacto de los ransomware en oficinas de la facultad de administración, finanzas e informática.

Objetivos Específicos

- Revisar bases teóricas de seguridad informática que permitan determinar factores críticos inherentes al ransomware.
- Analizar las situaciones de riesgo en base a la experiencia del especialista al que se le aplicó la entrevista.
- Proponer estrategias para prevenir ataques y mejorar la recuperación en caso de incidentes similares.

LÍNEA DE INVESTIGACIÓN Y ARTICULACIÓN DEL TEMA

Este trabajo de estudio de caso, está orientado y alineado con la línea de investigación de: Sistemas de información y comunicación, emprendimiento e innovación que además esta conjuntamente relacionado con la sublínea de investigación: Redes y tecnologías inteligentes de software y hardware.

Así mismo, este caso de estudio permite una articulación con la práctica pre profesional realizada en el Gobierno Autónomo Descentralizado de la parroquia Los Ángeles del cantón Ventanas, puesto que se desarrollaron actividades de soporte tecnológico orientadas a mejorar la seguridad informática de equipos de cómputo que fueron comprometidos con ransomware afectando de forma operativa a la institución; además, permitió demostrar habilidades adquiridas en la formación universitaria entorno a la mitigación y recuperación de esos incidentes.

Es importante mencionar que además la sub línea de investigación se la vincula estrechamente con la actividad secundaria que realizaba relacionada con mantenimiento de sistemas operativos, computadoras, impresoras y demás infraestructura tecnológica básica.

MARCO CONCEPTUAL

Seguridad de la información

La seguridad de la información es un campo multidisciplinario que permite enfocarse en la protección y confidencialidad, así como también la integridad y disponibilidad de datos e información. Es un concepto que abarca la aplicabilidad de políticas, procedimientos y tecnologías para prevenir los accesos no autorizados. La importancia radica dependencia creciente que tienen las organizaciones y la sociedad en el ámbito de la información digital, así como en sus riesgos de pérdida de dicha información. (James Michael Stewart, 2021)

La seguridad de la información está basada en fundamentos clave de resguardo de la información y la protección de activos digitales, así como la continuidad de operaciones de las organizaciones basadas en cumplimientos normativos, pues implica evaluación de amenazas potenciales que pueden suceder en cualquier momento y las medidas para mitigar y recuperarse; por lo que es fundamental la capacitación del talento humano en relaciona a las buenas prácticas institucionales de detección temprana de intrusiones. (José María Pisa, 2022)

Además, es importante mencionar que la seguridad de la informática es un proceso en constante evolución y renovación puesto que, las amenazas cibernéticas y los también evolucionan con el pasar del tiempo. Por lo que, las empresas deben estar siempre actualizadas con las mejores prácticas relacionadas con técnicas de seguridad, así como es importante realizar evaluaciones riesgos y auditorías de seguridad de forma periódica. (María José Erta, 2018)

La implementación de forma eficiente de la seguridad de la información no solamente protege los datos confidenciales de una empresa sino también permite fortalecer su reputación ya que la seguridad de la información se convierte en uno de los componentes fundamentales para el éxito seguro de cualquier organización. (Nicanor García, 2020)

(Schneier, Secrets and Lies: Digital Security in a Networked World, 2020) Indica que, la concienciación y la capacitación del recurso humano es muy fundamental en relación a la seguridad informática estas son aspectos esenciales para mitigar los riesgos

considerando planes de capacitación en este caso para la facultad a sus administrativos estudiantes y docentes, la gestión de incidente debe incluir métricas claras para poder pretender respuestas eficaces ante amenazas con investigaciones forenses que permitan determinar sus alcances y causales.

El trabajo colaborativo y el de compartir información con otras organizaciones son cruciales en estos temas de amenazas cibernéticas ya que puedes tener el beneficio de las experiencias de sus similares que pueden hacer empresas de sector público y privadas permitiendo estar al tanto de las últimas amenazas surgidas y cuáles serían sus mejores prácticas para mitigarlas. La seguridad informática en las instituciones de educación superior requiere una combinación de políticas y tecnología, así como de conciencia y colaboración para proteger y mantener la confianza de todas las partes interesadas. (Schneier, Secrets and Lies: Digital Security in a Networked World, 2020)

El dañino ransomware

El ransomware es una forma de virus dañino de tipo o malware que se ha convertido en una de las amenazas más significativas y peligrosas en el mundo de la seguridad de la información el impacto que tiene en todos los ámbitos pesa pues es conocido que ha logrado destruir grandes cantidades de datos en corporaciones y entidades de gobierno. (Holloway, 2022)

Está elaborado como un tipo de software malicioso diseñado para bloquear el contenido de los archivos y además el acceso a los sistemas informáticos cifrando su contenido hasta que la víctima pague un rescate, es conocido que se puede pagar hasta en criptomonedas para lograr recuperar el acceso y el contenido de los archivos. Los delincuentes del internet que desarrollan los ransomware utilizan diferentes técnicas para propagar este virus malicioso que incluye desde correos electrónicos descargas maliciosas ataques dirigidos y exploits de vulnerabilidades. (José María Pisa, 2022)

Impacto del ransomware

Según (Anderson, Security Engineering, A Guide to Bulding Dependable Distributed Systems, 2021) El impacto que tiene el ransomware cuando este ha afectado a una organización puede ser devastador. Opina además (López-Diéguez, 2020) que, las víctimas pueden perder el acceso a los datos críticos de la organización estos pueden ser datos privados también de su vida personal lo que puede resultar en la interrupción de las operaciones daños a la reputación pérdida financieras y demás daño a infraestructuras que están conectadas y dependen de sistemas de información.

En algunos casos, es conocido que los ataques de ransomware han conducido al cierre de empresas a nivel mundial por la pérdida de sus datos como fotografías documentos hojas de cálculo bases de datos financieras, así como también se han efectuado muchos pagos debido a rescates y esto implica pérdida de dinero para empresas pequeñas. (Amutio, 2020) Indica que, es conocido que puede generar estrés y ansiedad en las víctimas pues estos no siempre tienen copias de seguridad de los datos o información incluso luego de pagar un rescate por lo que puede tener además consecuencias emocionales duraderas para las personas que han sido víctimas de estos ataques ransomware. (Microsoft, 2021)

Prevención y mitigación

La prevención y mitigación del ransomware requiere de una combinación de conocimientos y habilidades técnicas, así como de educación al usuario en cuanto a utilización de sistemas y tipos de descarga y la preparación de incidentes que pueden ocurrir. (Bruce, 2020) en su libro, se indica que una de las medidas que pueden ser primarias es la utilización de software de seguridad actualizado dentro de equipos activos de la red esto es firewalls, sistemas de IPS IDS y sobre todo mantener una disciplina relacionada con copias de seguridad regulares fuera de línea replicadas en nubes privadas. La educación de todas las personas que intervienen en la organización es crucial para evitar caer en la trampa y descargar archivos maliciosos. Además de que es necesario mantener planes de recuperación rápida frente a incidentes ya parametrizados, que puedan incluir la capacidad de aislar rápidamente sistemas informáticos afectados con restauraciones rápidas de copias de seguridad confiables. (Schneier, Secrets and Lies: Digital Security in a Networked World, 2020)

Es un aspecto crucial prevenir y mitigar los ransomware como tipo de amenaza cibernética para que se pueda evitar este tipo de amenazas y convertirse en víctima de ransomware las empresas y las personas deben implementar una forma combinada medidas tecnológicas de seguridad de la información que permitan educar a las personas y mantener respuestas planificadas a incidentes. (Schneier, Secrets and Lies: Digital Security in a Networked World, 2020)

Educar a los usuarios es un papel crucial en todo aspecto orientado a la seguridad de la información y el ransomware no es la excepción, los usuarios deben de ser capacitados para reconocer posibles amenazas de phishing que llegan como correos electrónicos sospechosos o enlaces que no han sido solicitados a través de conocidos; también hay que ser conscientes de que existen riesgos asociados con descargas de archivos adjuntos de correos y redes sociales. Una capacitación planificada en seguridad informática puede ayudar a tener una postura fortalecida en la organización ya que se involucran a los empleados en la protección los activos digitales. (Schneier, Secrets and Lies: Digital Security in a Networked World, 2020)

Desde una visión técnica es absolutamente fundamental mantener actualizado todo software de seguridad es decir antivirus y anti malware con sus bases de datos al día así como mantener el sistema operativo con las últimas actualizaciones y una configuración adecuada de firewall interno y perimetral reducirían el riesgo acompañado de una política de copias de seguridad periódicas para garantizar la disponibilidad de datos frente a un ataque de ransomware (Doctorow, 2021).

Además de mantener medidas preventivas, es necesario establecer controles claros que permitan detecciones tempranas, su contención y eliminación de ransomware en caso de ser atacados. También son importantes los protocolos para comunicaciones internas y externas. Tener una capacidad de respuesta de manera ágil puede ayudar a reducir la vulnerabilidad ante estas amenazas y acelerar la recuperación de sistemas que hayan sido afectados. (María José Erta, 2018)

Evolución del ransomware

El ransomware ha logrado una evolución con el transcurrir del tiempo, y se ha podido adaptar a diferentes tipos de defensas de seguridad, adoptando cada vez nuevas tácticas lograr sus beneficios. Esto incluye esquemas de funcionamiento de ransomware como servicio (RaaS), donde los criminales de la red o hackers o hasta usuarios comunes alquilan o comprar utilidades de ransomware completos, facilitando así su distribución y aumentando la amenaza por su cantidad de ataques. (kaspersky, 2021)

Su evolución ha sido notable desde sus inicios hasta su actualidad, exponiéndose como una de las amenazas actuales más peligrosas y sofisticadas en el contexto de la ciberseguridad. En sus inicios, el ransomware solía de acción simple y directo, bloqueando el acceso los archivos y sistemas, cifrándolos y exigiendo pagos por su rescate y restablecimiento del acceso. Sin embargo, ha transcurrido el tiempo y se han presentado mejoras, donde los atacantes cuentan con mejores técnicas y estrategias rentables. (Joseph Muniz, 2023)

Una tendencia significativa en su evolución, es la nueva forma de modelo de negocio conocido como ransomware-as-a-Service (RaaS). Este modelo permite que los ciberdelincuentes puedan comprar o alquilar kits completos de software ransomware, lo que les permite lanzar ataques de gran escala e impacto. (Evan Greer, 2022)

Existe otra forma preocupante de ataque de doble extorsión, donde el ciberdelincuente amenaza con publicar datos sustraídos además de cifrarlos, aumentando la presión sobre sus víctimas para que estos paguen por el rescate grandes sumas. Esta estrategia utilizada no solo amplía su impacto, sino que también genera preocupaciones adicionales en el contexto de la protección de datos y la privacidad. (Holloway, 2022)

Desafíos futuros a los que nos obliga el ransomware

A medida que la tecnología se desarrolle, los problemas de ransomware aumentaran. Se espera que los ciberdelincuentes sigan desarrollando variante de ransomware nuevas más sofisticadas y más difíciles de detectar lo que requiera que las organizaciones conserven sus defensas actualizadas y adopten un enfoque proactivo y tomen medidas para detectar y remediar las amenazas. (S.L., 2021)

Los retos futuros que diseña el ransomware son diversos y graves y requieren respuestas sólidas y sostenidas por parte de individuos, organizaciones y la comunidad de ciberseguridad en general. (S.L., 2021)

Uno de los ´principales desafíos es el desarrollo y la mejora continua de las variantes de ransomware. Los ciberdelincuentes desarrollan constantemente nuevos métodos y tácticas para eludir las medidas de seguridad y maximizar la eficacia de sus ataques. (S.L., 2021)

Estos ataques no solo cifran los datos de las víctimas, sino que también amenazan con publicar información confidencial en línea a menos que se pague un rescate. Estas tácticas pueden tener consecuencia devastadora para la reputación y la privacidad de las víctimas y plantear cuestiones técnicas y legales sobre como satisfacer las demandas laborales de los atacantes. (Holloway, 2022)

Otra preocupación importante es la creciente amenaza que representa la ransomware para la infraestructura crítica y los servicios gubernamentales. Las interrupciones en los servicios esenciales pueden dañar a la sociedad a poner vidas en riesgo, lo que detecta la necesidad de fortalecer la ciberseguridad en estos sectores y adoptar un enfoque legal para minimizar los riesgos. (Holloway, 2022)

Además, el aumento de la conectividad y la proliferación de dispositivos IoT (Internet of Things) crean nuevas oportunidades para los ciberdelincuentes para lanzar ataques de ransomware. Los dispositivos IoT, que incluyen desde cámaras de seguridad y termostatos hasta dispositivos médicos y automóviles conectados, a menudo carecen de las medidas de seguridad adecuadas y pueden servir como puntos de entrada vulnerables en las redes corporativas y domésticas. La seguridad de los dispositivos IoT es fundamental para proteger contra el ransomware y otras amenazas cibernéticas emergentes. (Holloway, 2022)

La falta de cooperación y coordinación internacional también plantea un desafío importante en la lucha contra el ransomware. Dado que los ciberdelincuentes operan en un entorno global y pueden lanzar ataques desde cualquier parte del mundo, la cooperación eficaz entre gobiernos organismos encargados de hacer cumplir la ley, empresas y organizaciones internacionales es esencial. (Holloway, 2022)

Los desafíos del ransomware del futuro son diversos y complejos, y requerirán colaboración y una respuesta multifacética. Solo a través de una respuesta unificada y coordinada podemos esperar combatir eficazmente la creciente amenaza del ransomware. (McGraw, 2022)

El ransomware representa una grave amenaza para personas, empresas y gobiernos de todo el mundo. Su impacto puede ser devastador, pero una combinación de, medidas técnicas, educación de los usuarios y preparación para incidentes puede reducir los riesgos asociados con ellos y reducir la efectividad de este tipo de ataques. (McGraw, 2022)

Aspectos técnicos y detección de ransomware

La detección de ransomware es un proceso importante para prevenir ataques cibernéticos. Este proceso implica identificar y detectar malware, como ransomware ingrese a un sistema o red. Esto se hace monitoreando actividades sospechosas, escaneando amenazas conocidas y analizando registro del sistema y otras fuentes de datos en busca de anomalías que podrían indicar un ataque. (Doctorow, 2021)

Existen varios métodos para detectar ransomware. Uno de ellos es el análisis de archivos estáticos, que implica examinar los archivos en busca de características típicas de ataques de ransomware. Otro método es utilizar una lista llena de extensiones de archivos comunes utilizados por ransomware. Las técnicas de phishing, como los archivos de señuelo, también pueden resultar útiles para detectar ransomware. Estos archivos actúan como cebo para atraer ransomware, lo que garantiza una detención temprana. (Doctorow, 2021)

Tabla 1. Aspectos técnicos y la descripción relacionados con ransomware

Aspecto Técnico	Descripción
Análisis de comportamiento	Monitoreo de actividades sospechosas o inusuales en el sistema, como cambios masivos de archivos o acceso a recursos inusuales.
Firma de malware	Utilización de bases de datos de firmas de ransomware conocidas para identificar archivos o procesos maliciosos.
Análisis heurístico	Detección basada en el comportamiento y características generales del ransomware, en lugar de firmas específicas.
Listas blancas y negras	Implementación de listas de aplicaciones permitidas (blancas) y prohibidas (negras) para controlar qué programas pueden ejecutarse en el sistema.
Control de acceso a archivos	Restricción de acceso a archivos importantes y sensibles para prevenir la modificación no autorizada por parte del ransomware.
Detección de cifrado inusual	Monitorización de patrones de cifrado de archivos inusuales o anómalos que podrían indicar actividad de ransomware.
Análisis de tráfico de red	Inspección de patrones de comunicación típicos de ransomware, como intentos de conexión a servidores de comando y control (C&C) o transmisión de datos cifrados.
Monitoreo de cambios en el registro	Seguimiento de modificaciones en el registro del sistema que podrían ser realizadas por el ransomware para persistir en el sistema o modificar su comportamiento.
Protección de puntos finales	Implementación de soluciones de seguridad específicas para proteger dispositivos finales, como antivirus avanzados o soluciones de detección y respuesta de endpoint (EDR).
Actualizaciones de seguridad	Mantenimiento regular del sistema y de las aplicaciones actualizadas para cerrar posibles brechas de seguridad utilizadas por el ransomware para infiltrarse en el sistema.

Fuente: (Doctorow, 2021)

Tabla 2. Algunas posibles estrategias que podrían ayudar en la recuperación de un sistema afectado por ransomware

Estrategia o Comando	Descripción
Restaurar copias de seguridad	Recupera archivos y datos desde copias de seguridad previamente creadas y almacenadas fuera del alcance del ransomware.
Utilizar herramientas de desencriptación	Algunas organizaciones de seguridad y fabricantes de antivirus proporcionan herramientas de desencriptación gratuitas para ciertos tipos de ransomware.
Analizar sistemas en busca de vulnerabilidades	Escanear el sistema en busca de vulnerabilidades que puedan haber sido explotadas por el ransomware y corregirlas para prevenir futuros ataques.
Investigar el tráfico de red	Analizar el tráfico de red en busca de comunicaciones maliciosas o conexiones a servidores de comando y control (C&C) para identificar la fuente del ransomware.
Restaurar configuraciones de fábrica	Restaurar los dispositivos afectados a la configuración de fábrica para eliminar el ransomware y comenzar de nuevo con un sistema limpio.
Analizar registros del sistema	Revisar los registros del sistema en busca de actividad inusual o registros de eventos asociados con el ransomware para comprender mejor cómo se infiltró y propagó.
Desconectar sistemas de la red	Aislar los sistemas infectados desconectándolos de la red para evitar la propagación adicional del ransomware y proteger otros sistemas conectados.
Colaborar con expertos en seguridad	Buscar ayuda de profesionales de seguridad informática o agencias gubernamentales para asistencia en la recuperación y análisis forense del ransomware.
Restaurar desde imágenes de sistema	Restaurar los sistemas afectados desde imágenes de sistema o instantáneas previas almacenadas en dispositivos de almacenamiento externos o en la nube.
Implementar soluciones de seguridad adicionales	Reforzar la seguridad del sistema mediante la implementación de soluciones adicionales, como firewalls avanzados, sistemas de detección de intrusiones, etc.

Fuente: (María José Erta, 2018)

Estos comandos aquí descritos y las demás acciones pueden variarse según la naturaleza o característica específica del ransomware y circunstancias del ataque realizado, sin embargo, proporcionan un punto de partida a tener en cuenta para la recuperación y mitigación de posibles daños causados por el ransomware.

Tabla 3. Herramientas más comunes y eficaces para la recuperación de sistemas afectados por ransomware, junto con sus pros y contras:

Herramienta	Descripción	Pros	Contras
ShadowExplorer	Una herramienta que permite acceder y recuperar versiones anteriores de archivos utilizando las instantáneas del volumen.	- Interfaz fácil de usar. - Permite recuperar archivos sin necesidad de pagar el rescate.	- Depende de la disponibilidad de instantáneas del volumen. - No es efectiva si el ransomware las elimina.
Recuva	Un software de recuperación de datos que puede ayudar a restaurar archivos borrados accidentalmente.	- Gratuito y fácil de usar. - Puede recuperar archivos incluso después de ser eliminados por el ransomware.	- Puede no ser efectivo si los archivos están cifrados de manera irreversible.
PhotoRec	Una herramienta de recuperación de archivos de código abierto que puede recuperar más de 480 tipos de archivos diferentes.	- Gratuito y de código abierto. - Soporta una amplia gama de tipos de archivos.	- Interfaz de usuario basada en línea de comandos, que puede resultar complicada para algunos usuarios.
TestDisk	Un programa de recuperación de datos de código abierto que puede ayudar a recuperar particiones perdidas y reparar tablas de particiones.	- Gratuito y de código abierto. - Puede recuperar particiones perdidas y restaurar la funcionalidad del disco.	- Interfaz de usuario basada en línea de comandos. - Requiere conocimientos técnicos para su uso adecuado.
R-Studio	Una suite de recuperación de datos con una amplia gama de características para recuperar archivos de discos dañados o formateados.	- Interfaz de usuario intuitiva. - Puede recuperar datos de discos dañados, formateados o cifrados.	- No es gratuito. - La versión completa puede ser costosa.

Fuente: (McGraw, 2022)

Estas herramientas ofrecen diversas opciones para intentar recuperar datos afectados por ransomware, pero es importante tener en cuenta que su efectividad puede variar dependiendo de varios factores, como la naturaleza y la severidad del ataque de ransomware, así como el estado de los datos afectados. Además, ninguna herramienta puede garantizar la recuperación total en todos los casos, por lo que es importante

mantener copias de seguridad actualizadas como parte de una estrategia de protección contra el ransomware.

Qué debe hacer una institución si tiene ransomware en sus equipos

Teniendo en cuenta la posibilidad de que una institución se vea afectada por el malware llamado ransomware es muy grande debido a que los ciberdelincuentes buscan robar la información de la institución para hacer de aquello un lucro impropio por lo que para prevenir esa situación se debe tener presente varias instrucciones a seguir para evitar el daño y robo de la información. Como punto número uno es muy relevante localizar y aislar todos los sistemas que están infectados para así evitar la propagación del ransomware. Realizar esta acción implica un análisis de registros del sistema a través de varias herramientas de seguridad una de ellas es el antivirus dado a que gracias a este software se puede identificar los sistemas afectados. (Holloway, 2022)

Ya una vez realizada la acción de aislar todos los sistemas infectados, la institución debe diseñar imágenes de disco de esos sistemas para después proceder a hacerles su respectivo análisis. Con ayuda de este análisis se podrá entender cómo se filtró ransomware en los sistemas y que otros daños causo en los equipos informáticos de la institución. (Nicanor García, 2020)

Adicional a los pasos técnicos ya antes mencionado, es importante que la institución informe de manera transparente con el respaldo de sus empleados y el público presente dé a conocer sobre el problema ocurrido. Ya que esto permite reducir la mala reputación de la institución y a su vez ayuda a que la parte interesada a tomar una decisión para dar una solución al problema. (kaspersky, 2021)

Si una institución se ve atacada por el malware ransomware lo que tiene que hacer es dar una respuesta rápida al ataque para que se reduzca el daño que están tratando de

hacer a la institución siguiendo los pasos ya antes mencionados en los párrafos anteriores para así tener conocimientos de lo que se debe de hacer. (Schneier, Secrets and Lies: Digital Security in a Networked World, 2020)

Cómo contrarrestar los daños causados por el ransomware

Enfrentarse al ransomware a través de los daños que ha ocasionado involucra varias instrucciones que incluyen la prevención de sufrir ataques severos por parte de los que administran el ransomware, responder de manera inmediata al ataque incluye la implementación de seguridades robustas tales como la regularización de copias de seguridad informática, tener actualizados los programas, el sistema operativo, el parcheo de la seguridad de datos en la nube y por último el almacenamiento interno. (kaspersky, 2021)

Dado el caso de que, si el ataque del ransomware fue de manera severa, una respuesta inmediata al aislar todos los sistemas infectados desconectando las redes, el escáner y eliminando todos los archivos maliciosos a través de un antivirus es lo mejor para así tratar de salvar la información que quisieron robar. Después de aquella sugerencia lo mejor sería restaurar los archivos desde una copia de seguridad o utilizar alguna herramienta para descripta los archivos. (Microsoft, 2021)

Contrarrestar el ransomware es lo mejor que se puede hacer debido a que si no se hace eso ellos pueden robar en absoluto toda la información de la institución y poner en peligro el futuro de la misma por lo que para evitar aquello es mejor contrarrestar el ransomware siguiendo los pasos ya mencionados. (kaspersky, 2021)

Estrategias para prevenir ataques de ransomware

Según lo mencionado por (kaspersky, 2021) nos informa que, evitar los ataques del ransomware es algo fundamental para la seguridad cibernética, ya que la estrategia de prevenir estos ataques se integra la realización de hacer copias de seguridad de todos los datos de la institución usando la seguridad Zero Turts debido a que esto puede ayudar a restaurar los sistemas en caso de que el ataque del ransomware sea severo, también se debe agregar diciendo que si se protege los datos contra las vulneraciones de los ataques sería lo mejor ya que esto implica a no confiar en nada de lo que este adentro o fuera de la red sin ninguna verificación.

Por otro lado, la formación del usuario es una parte fundamental para poder evitar ataques del ransomware, ya que los usuarios deben ser adecuados para poder detectar todos los ataques que hacen como por ejemplo no revisar correos sospechosos o descargar archivos de fuentes desconocidas. (Holloway, 2022)

Evitar los ataques de ransomware es una función que requiere de un enfoque integral que lleva en cuenta tanto las medidas técnicas como las educativas. Todas las medidas técnicas son primordiales para fortalecer las infraestructuras contra las posibles amenazas. Dado un ejemplo de aquellos sería el respaldo de información que protege la vulnerabilidad de los ataques del ransomware. (José María Pisa, 2022)

También un enfoque de seguridad Zero Trust es de suma efectividad. Ya que esto implica en no confiar en nadie dentro de la red ya que eso ayuda aprevenir ataques del ransomware debido a que se restringe el acceso a los sistemas y datos dando el acceso solo a aquellos que en verdad deben tener esa información. (José María Pisa, 2022)

La prevención de ataques de ransomware es una responsabilidad multifacética que necesita un enfoque holístico. Al desarrollar una combinación de medidas técnicas y

educativas, por medio de las organizaciones pueden benefician la postura de la seguridad y reducir el riesgo de sufrir un ataque de ransomware. Esto no sólo protege los sistemas y datos de la organización, sino que también minimiza el tiempo de inactividad y los costos asociados con la recuperación de un ataque de ransomware. En si la inversión en la prevención de ransomware se puede considerar como una estrategia de negocio prudente y especifica que ayuda con la prevención del robo de información. (Schneier, Secrets and Lies: Digital Security in a Networked World, 2020).

MARCO METODOLÓGICO

Este estudio se enfoca en comprender las estrategias de recuperación utilizadas para mitigar el impacto de los ataques de ransomware en las oficinas de la facultad de administración, finanzas e informática. Se adopta un enfoque cualitativo para explorar en profundidad las percepciones, experiencias y prácticas relacionadas con la seguridad cibernética en este contexto específico.

La investigación será de naturaleza documental, cualitativa y experimental ya que se busca comprender y describir fenómenos complejos y subjetivos, como las estrategias de recuperación ante los ataques de ransomware, desde la perspectiva de los participantes involucrados en el estudio.

Se utilizará la técnica de entrevistas en profundidad para recopilar datos. Estas entrevistas permitirán explorar a fondo las experiencias, conocimientos y recomendaciones de expertos en seguridad cibernética y gestión de la información en el ámbito académico.

El instrumento principal será la "guía de entrevista", la cual contendrá preguntas y temas diseñados para guiar la conversación con los expertos. Esta guía se desarrollará considerando aspectos clave como las estrategias de recuperación, medidas de seguridad implementadas, desafíos enfrentados y lecciones aprendidas.

Se seleccionarán o crearán heurísticas específicas para guiar la evaluación de las estrategias de recuperación ante ransomware. Estas heurísticas servirán como principios generales de diseño y prácticas recomendadas para evaluar la eficacia y la eficiencia de las medidas implementadas.

Procedimientos de Investigación:

- Selección del participante: Se seleccionará al experto en seguridad cibernética y gestión de la información dentro del ámbito académico.
- Entrevistas en profundidad: Se llevará a cabo la entrevista individual al participante, utilizando la guía de entrevista como marco de referencia.
- Análisis de datos: Se analizarán los datos recopilados mediante técnicas cualitativas, incluyendo el análisis de contenido y el análisis comparativo.

- Interpretación y discusión: Se discutirán los hallazgos con el experto en diseño web y seguridad cibernética, comparando y contrastando las estrategias de recuperación identificadas y analizando su efectividad en la prevención y gestión de ataques de ransomware.

Además, se obtendrá el consentimiento informado del participante antes de llevar a cabo la entrevista. Todas las prácticas de investigación se realizarán de acuerdo con los principios éticos establecidos en el ámbito académico.

Nombre del Entrevistado Master. Harry Saltos Viteri

Lugar de Trabajo: UTB - FAFI

Experiencia: Ingeniero en sistemas con más de 20 años de experiencia en Tecnologías de la información, ha ocupado cargos en instituciones públicas y privadas desde 1996 en áreas relacionadas a la ingeniería, redes, seguridades y Linux, desarrollador de sistemas.

Entrevista con el objetivo: De recoger buenas prácticas y experiencias en el contexto de estrategias de recuperación frente al Impacto de los ransomware en oficinas de la facultad de administración finanzas e informática de la Universidad Técnica de Babahoyo.

RESULTADOS

El enfoque principal de la entrevista realizada como instrumento de investigación recoge que, se debe ser integral, esto implica una combinación de capacitación y concienciación del personal y los usuarios sobre buenas prácticas que deben existir en la institución, además de implementarse soluciones que permitan detener amenazas y para esto usar firewalls actualizados, software de antivirus y antimalware, además estrategias de segmentación de redes para limitar propagación de las infecciones.

Así mismo, se ha recogido que además, como medida de respaldo y recuperación de datos, se puede implementar una estrategia de almacenamiento de copias de seguridad automatizadas desde el programador de tareas para que genere copias a una carpeta compartida y estas las sincronice a la nube para mantener redundancia de los datos críticos de la facultad y que puedan estar fuera del alcance de algún ransomware.

Recomienda el experto que el almacenamiento puede ser la nube o servidores externos con sistemas operativos del tipo Linux. Además, es esencial realizar pruebas periódicas como ejercicios de recuperación de datos en caso de un incidente de ransomware.

En el contexto de evaluar y actualizan regularmente políticas de seguridad informática y demás protocolos de respuesta a incidentes, se ha obtenido que, en publicas existen normas de control interno que son exigidas por contraloría general del estado, por lo que el departamento de sistemas de la institución debe tener unas políticas aprobadas donde se refleje que hacer en caso de alguna amenaza y para la continuidad de las operaciones como lo son los planes de contingencia requeridos por ese organismo del estado.

El asunto con evaluar estas políticas y protocolos es su efectividad, ya que en muchos lugares solo por cumplir, tienen un documento que no causa efectos y no se aplica y ni se lo socializa. Por lo que considero es importante tener políticas personalizadas para cada organización y que estas permitan mitigar alguna amenaza.

En cuanto a algún plan de acción inmediato y que estrategias emplearía para solucionar la situación minimizando impactos y las pérdidas de datos críticos basados en la experiencia del experto, este recomienda:

- Aislar el equipo y así evitar su propagación y de ser el caso notificar a los directivos pertinentes para que se realice la gestión de recuperación y mitigación.
- Aplicación de mecanismos forenses para copiar los datos en una imagen para trasladarla a otro sistema operativo distinto en arquitectura para que no se active la amenaza, luego tratar de recuperar con software especializado los datos y si se tienen copias de seguridad restaurarlas restaurar para mantener una continuidad del negocio.
- En muchos casos también se debe trabajar con abogados especializados en este tipo de incidentes para permitan una evaluación del alcance del daño en términos legales y determinar el mejor camino a seguir.

Las lecciones aprendidas relacionadas con ransomware, para ajustar estrategias de seguridad y recuperación serían según el entrevistado:

No perder el tiempo tratando de recuperar lo que ya está infectado, en mi experiencia particular solo el 2% se ha podido recuperar y ha sido una perdida grandísima de tiempo, por lo que es importante evaluar el tiempo invertido versus el costo de lo que se está perdiendo, sobre todo si se tiene backups y no es tan grave, es posible que un técnico pueda perder mucho tiempo en desencriptar.

También se indica que no hay que esperar a que ocurra, lo mejor es prevenir porque el impacto es muy negativo y la mayoría de las veces irreversible, por lo que la capacitación del personal es crucial, de esa forma es que se mejoran las medidas de seguridad cibernética y además aumentado la frecuencia de copias de seguridad.

DISCUSIÓN DE RESULTADOS

Se ha analizado el siguiente párrafo, el cual se analizará la postura crítica del autor Schneider el cual indica que:

La prevención y mitigación del ransomware requiere de una combinación de conocimientos y habilidades técnicas, así como de educación al usuario en cuanto a utilización de sistemas y tipos de descarga y la preparación de incidentes que pueden ocurrir. Una de las medidas que pueden ser primarias es la utilización de software de seguridad actualizado dentro de equipos activos de la red esto es firewalls, sistemas de IPS IDS y sobre todo mantener una disciplina relacionada con copias de seguridad regulares fuera de línea replicadas en nubes privadas. La educación de todas las personas que intervienen en la organización es crucial para evitar caer en la trampa y descargar archivos maliciosos. Además de que es necesario mantener planes de recuperación rápida frente a incidentes ya parametrizados, que puedan incluir la capacidad de aislar rápidamente sistemas e informáticos afectados con restauraciones rápidas de copias de seguridad confiables.

Es un aspecto crucial prevenir y mitigar los ransomware como tipo de amenaza cibernética para que se pueda evitar este tipo de amenazas y convertirse en víctima de ransomware, las empresas y las personas deben implementar una forma combinada medidas tecnológicas de seguridad de la información que permitan educar a las personas y mantener respuestas planificadas a incidentes.

Y contrastando con la opinión del autor de este caso de estudio, más la opinión del entrevistado, se analiza que:

Es necesario implementar sobre todo estrategias de prevención ya que esto debería ser un estándar en el caso de los ransomware por lo que su mitigación es muy compleja y es necesario tener equipos de vanguardia actualizados que permitan la detección

temprana de este tipo de amenaza, además los criterios son muy coincidentes con el autor Schneider en esta discusión de resultados pues también se considera necesaria mantener planes de recuperación en todas las instancias de la institución y por qué no de la facultad de administración finanzas e informática para hacerle frente a incidentes que podrían ocurrir en el evento de ser atacados por un ransomware.

CONCLUSIONES

Prevenir y mitigar al ransomware es una combinación de educación y conocimientos técnicos; se han analizado estrategias de recuperación en este documento, así como se han recogido experiencias de profesionales y lo importante de esto es prevenir y estar preparados cuando un incidente de estos ocurra.

Es una necesidad mantener una capacitación en la institución para los cuidados en la navegación, así como la utilización de medios extraíbles, esto debe ser una política generalizada, para evitar caer en trampas de descargas y resaltar la concienciación sobre la importancia de proteger los datos.

Mantener planes para una recuperación rápida frente a algún incidente es necesario, de este caso de estudio se recoge además la inquietud de algún maestro que le preocupaba el tema en relación a que, si ya ha sucedido o si ya tienen este inconveniente en la facultad, sin embargo este análisis ha permitido determinar y concluir que es más importante tener una política de prevención, acompañado de una estrategia para recuperación y reducción del impacto.

Implementar estrategias para prevención, incluyendo equipos y software adecuados y actualizados para una detección oportuna ante estas amenazas, reduciría el impacto, sin embargo, esto debe venir de una alta dirección de la institución, puesto que en la facultad motivo de este análisis son ejecutores de órdenes y lineamientos de una dirección de sistemas.

RECOMENDACIONES

Se recomienda al decano de la facultad hacer las gestiones pertinentes que les permita prevenir posibles incidentes relacionados con pérdidas de información por motivos externos como el ransomware, además de delegar alguna campaña de concienciación y educación entorno a la utilización de descargas de archivos y compartición de archivos usando medios como memorias extraíbles.

Así mismo se recomienda a la dirección de sistemas de la Universidad donde pertenece la facultad de administración, finanzas e informática mantener planes de recuperación rápida frente a incidentes y pérdidas de información por motivos de ransomware y otros factores de ser el caso.

A la dirección de sistemas de la institución se recomienda preparar algún tipo de políticas o lineamientos para reducir riesgos ante contenidos maliciosos que pueden ser descargados y compartidos por los usuarios.

REFERENCIAS BIBLIOGRÁFICAS

Amutio, M. A. (2020). *La Amenaza Hacker: Guía para la defensa de la información en el mundo digital.* Malaga: Anaya Multimedia.

Anderson, R. (2021). *Security Engineering, A Guide to Bulding Dependable Distributed Systems.* Indianápolis: Wiley.

Anderson, R. (2021). *Security Engineering: A Guide to Bulding Dependable Distributed Systems.* Indianápolis: Wiley.

Bruce, S. (2020). *Criptografía La ciencia de la seguridad de la información.* Madrid: Alianza Editorial.

Doctorow, C. (2021). *Little Brother.* New York: Tor Teen.

Evan Greer, J. K. (2022). *Zero Trust Security: The Definitive Guide.* O'Reilly Media.

Holloway, M. P. (03 de Mayo de 2022). *Cómo prevenir los ataques de ransomware*. Cómo prevenir los ataques de ransomware: https://www.cloudflare.com/es-es/learning/security/ransomware/how-to-prevent-ransomware/

James Michael Stewart, M. C. (2021). *Seguridad de la Información: Preparación para la Certificación CISSP.* Chicago: Pearson.

José María Pisa, J. M. (2022). *Seguridad de la Información: Guía Práctica.* Madrid: RA-MA Editorial.

Joseph Muniz, P. K. (2023). *Cybersecurity for Dummies.* John Wiley & Sons.

kaspersky. (24 de julio de 2021). *Cómo reducir al mínimo las consecuencias de un ataque de ransomware corporativo.* Cómo reducir al mínimo las consecuencias de un ataque de ransomware corporativo.: https://www.kaspersky.es/blog/ransomware-attack-what-to-do/24774/

López-Diéguez, R. (2020). *Ciberguerra: La nueva realidad de la geopolítica.* Madrid: Deusto.

María José Erta, J. B. (2018). *Seguridad Informática: Conceptos Básicos.* Maracaibo: Marcombo.

McGraw, G. (2022). *Sotfware Security: Building Security in.* Boston: Addison -Wesley Professional.

Microsoft. (17 de Septiembre de 2021). *Tres pasos para prevenir y recuperarse del ransomware*. Tres pasos para prevenir y recuperarse del ransomware: https://news.microsoft.com/es-xl/tres-pasos-para-prevenir-y-recuperarse-del-ransomware/

Nicanor García, J. M. (2020). *Introducción a la Seguridad Informática.* Madrid: Ra-Ma Editorial.

S.L., J. C. (12 de marzo de 2021). *Mejores Prácticas Para Implementar Tecnologías Avanzadas De Detección De Ransomware*. Mejores Prácticas Para Implementar Tecnologías Avanzadas De Detección De Ransomware: https://helpransomware.com/es/contacto/

Schneier, B. (2020). *Secrets and Lies: Digital Security in a Networked World.* New York: Wiley.

ANEXOS

UNIVERSIDAD TECNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN FINANZAS E INFORMÁTICA

CARRERA DE SISTEMAS DE INFORMACIÓN

Entrevista con el objetivo: De recoger buenas prácticas y experiencias en el contexto de estrategias de recuperación frente al Impacto de los ransomware en oficinas de la facultad de administración finanzas e informática de la Universidad Técnica de Babahoyo.

Nombre del Entrevistado Master. Harry Saltos Viteri

Lugar de Trabajo: UTB - FAFI

Experiencia: Ingeniero en sistemas con más de 20 años de experiencia en Tecnologías de la información, ha ocupado cargos en instituciones públicas y privadas desde 1996 en áreas relacionadas a la ingeniería, redes, seguridades y Linux, desarrollador de sistemas.

Por favor responder abiertamente:

1. **¿Cuál considera usted que es el enfoque principal que permita una prevención y mitigación de ataques ransomware en una organización de educación superior?**

Debe ser un enfoque integral, esto implica la combinación de capacitación y concienciación del personal y los usuarios sobre buenas prácticas que deben existir en las organizaciones, deben de implementarse soluciones que permitan detener amenazas como firewalls actualizados, software de antivirus y antimalware, además de la segmentación de redes para limitar propagación de las infecciones por ransomware en caso de algún incidente. Además, es muy necesario mantener el software de SO actualizado con parches recientes de seguridad y realizar copias de seguridad a diario.

2. **¿Qué medidas aplicaría para respaldos y recuperación en el contexto de hacerle frente a posibles incidentes con ransomware?**

Como medida de respaldo y recuperación de datos, se puede implementar una estrategia de almacenamiento de copias de seguridad automatizadas desde el programador de tareas para que genere copias a una carpeta compartida y esta la sincronice a la nube para mantener redundancia de los datos críticos de la facultad y que puedan estar fuera del alcance de algún ransomware.

El almacenamiento puede ser la nube o servidores externos con sistemas operativos del tipo Linux. Además, es esencial realizar pruebas periódicas como ejercicios de recuperación de datos en caso de un incidente de ransomware.

3. **¿Cómo se pueden evaluar y actualizan regularmente las políticas de seguridad informática y demás protocolos de respuesta a incidentes para mantenerse actualizado con nuevas amenazas que van apareciendo de ransomware con técnicas cada vez variadas para ataques?**

En relación a instituciones públicas existen Normas de Control Interno que son exigidas por Contraloría General del Estado, por lo que considero que el departamento de sistemas de la institución debe tener unas políticas aprobadas donde se refleje que hacer en caso de alguna amenaza y para la continuidad de las operaciones como lo son los planes de contingencia requeridos por ese organismo del estado.

El asunto con evaluar estas políticas y protocolos es su efectividad, ya que en muchos lugares solo por cumplir, tienen un documento que no causa efectos y no se aplica y ni se lo socializa. Por lo que considero es importante tener políticas personalizadas para cada organización y que estas permitan mitigar alguna amenaza.

4. **De tener una incidencia de ataque ransomware, ¿cuál sería su plan de acción inmediato y que estrategias emplearía para solucionar la situación minimizando impactos y las pérdidas de datos críticos?**

Lo primero que haría es aislar el para evitar su propagación y de ser el caso notificar a los directivos pertinentes para que se realice la gestión de recuperación y mitigación. Si soy un técnico a ese equipo aislado le aplico mecanismos forenses para copiar los datos en una imagen para trasladarla a otro sistema operativo distinto en arquitectura para que no se active la amenaza, luego tratar de recuperar con software especializado los datos y si se tienen copias de seguridad restaurarlas restaurar para mantener una continuidad del negocio.

En muchos casos también se debe trabajar con abogados especializados en este tipo de incidentes para permitan una evaluación del alcance del daño en términos legales y determinar el mejor camino a seguir.

5. **¿Qué lecciones han aprendido de incidentes pasados de ransomware, y cómo han ajustado sus estrategias de seguridad y recuperación en base a esas experiencias?**

Las lecciones que he aprendido pues a no perder el tiempo tratando de recuperar lo que ya está infectado, en mi experiencia particular solo el 2% se ha podido recuperar y ha sido una perdida grandísima de tiempo, por lo que es importante evaluar el tiempo invertido versus el costo de lo que se está perdiendo, sobre todo si se tiene backups y no es tan grave, es posible que un técnico pueda perder mucho tiempo en desencriptar.

Como lecciones pasadas también se tienen que no hay que esperar a que ocurra, lo mejor es prevenir porque el impacto es muy negativo y la mayoría de las veces irreversible, por lo que la capacitación del personal es crucial, de esa forma es que se

mejoran las medidas de seguridad cibernética y además aumentado la frecuencia de copias de seguridad.

Babahoyo, 19 de febrero del 2024

Magister

Eduardo Galeas Guijarro

DECANO DE LA FACULTAD DE ADMINISTRACIÓN FINANZAS E INFORMÁTICA

En su despacho.

De mis consideraciones:

Yo: **GARCIA VEGA JUAN CARLOS**, con cédula de identidad 1207019132, estudiante de la carrera de Ingeniería Sistemas de Información matriculado en el proceso de titulación periodo Octubre 2023 – Marzo 2024, le solicito a usted de la manera más comedida se me permita realizar mi Caso de estudio en la FAFI con mi tema denominado **Análisis de estrategias de recuperación frente al impacto de los ransomware en oficinas de la Facultad de Administración Finanzas e Informática de la Universidad Técnica De Babahoyo** cual es requisito indispensable para poder titularme.

Esperando una respuesta favorable quedo de usted muy agradecido.

Del señor Decano muy atentamente

AUTORIZADO
19-02-24

Lcdo. Eduardo Galeas G.
DECANO

Juan García Vega

Juan Carlos García Vega

1207019132

RECIBIDO
UNIVERSIDAD TÉCNICA DE BABAHOYO
SECRETARIA FAFI
19-02-24. FECHA:
13:08 HORA: