Instructions

Build an attack case study report using this template. If you need help, refer to the instructional video.

There are five content slides plus a title slide in this template. You can receive up to 20 points for each content slide. You need 80 points to pass this assignment.

For your best chance of success, pick an attack or breach with enough information and data so that you will be able to report the required information.

Replace the red text on each slide with your information and change the text color to black or white, depending on the background. You can change the font size, if needed.

When your report is complete, delete this slide and save your file as a PDF to submit for review.

Case Study

Ramsonware

Aerolinea Colombiana Viva Air

Attack Category:
Ransomware

Ataque hecho por “Hive0091 ”, creador de “Ransomexx2”

1. El atacante ya tenia historial con estos tipos de ataque desde 2018 atacando a empresas del sector publico e internacionales como Ferrari

2. De alguna u otra manera el atacante pudo infringer la seguridad de la aerolinea, el dia 14 de marzo de 2022 se hizo una publicacion en un sitio WEB mediante la ruta cebolla donde se evidenciaban varios archivos con informacion sencible.

3. Se encontraron 18,25GB correspondiente a la informacion de 26,5 millones de clients, informacion como Nombres, numero de pasaporte, telefono y correo entre otros.

Sitio de la noticia: https://muchohacker.lol/2023/01/viva-air-leak-26-millones-de-datos-privados-de-clientes-de-la-aerolinea-de-bajo-costo-estarian-en-linea-desde-hace-nueve-meses/

Company Description and Breach Summary

Caida de Viva Air.

La aerolinea de bajo costo Viva Air, tenia una manejo de 46 rutas y 26 destinos, entre ellos 7 internacionales.

En febrero de 2023 se declare en quiebra, establecio que no contaba con las capacidades financieras ni operativas para continuar funcionando.

Unos de los motivos principales de su caida fue debido al fallo de ciberseguridad que tuvo hace un año sumado a varios problemas con los que venian previamente, tenia varias deudas las cuales no era capaz de cubrir por si sola, casi no contaba con capital debido a que su flota de aviones era alquilada y no propia.

Sumado a esto tuvo muchos problemas por la fuga de informacion que tuvo, dejando como ultima opcion la liquidacion de la misma.

Timeline

1

Event 1
El reconocido hacker Hive0091 logra infiltrarse en los sistemas de informacion de la aerolinea internacional, Viva Air, no se sabe exactamente como lo logro, muchos medios afirman que el software usado por Viva Air tenia deficit en la ciberseguridad

2

Event 2
Los atacantes piden dinero a cambio de la informacion a Viva Air, lamentablemente la aerolinea no cuenta con los recursos suficientes para pagar la extorsion debido a su delicado estado financiero

4

Event 3
El 14 de marzo del año 2022 fueron publicados varios archivos en un sitio web de la ruta cebolla que corresponden a datos robados de la aerolinea Viva Air, datos correspondientes a Nombre, numero de pasaporte, telefono, correo, etc...

5

Event 4
A mediados de febrero del año 2023 Viva Air se declara en quiebra ante la aeronautica civil, la gran cantidad de dificultades financieras y operativas la obligaron a liquidarse.

Vulnerabilities

In this box, provide an overall vulnerability summary.
Then provide a summary of 4 specific vulnerabilities for your case in the boxes below.

Vulnerability 1

Varios medios de comunicacion afirman que esto ocurrio debido al deficit tecnologico por parte de la aerolinea ya que contenia varios fallos importantes que atentaban contra la seguridad de la informacion

Vulnerability 2

El simple hecho de no contar con personal calificado en el area sabiendo que se trabajaba con informacion sensible es un actos de negligencia por parte de la aerolinea, dejando expuesta informacion personal

Vulnerability 3

La aerolinea no contaba con software dedicado a la proteccion en contra de archivos maliciosos o posibles fugas de informacion como antivirus, firewall, etc...

Vulnerability 4

Su personal nunca recibio capacitaciones enfocadas a la seguridad de los datos y la informacion, siendo un possible talon de aquiles del cual el atacante uso para cumplir su objetivo con fines economicos

Costs and Prevention

Costs

- 1. La informacion de un aproximado de 25,5 millones de clientes de la aerolinea quedo expuesta a gente con malas intenciones.
- 2. Cierre y caida total de la aerolinea Viva Air, dejando un aproximado de 46 rutas sin cubrir y dejando en situacion de desempleo a mucha gente.
- 3. Muchas personas que tenian vuelos programados con Viva Air perdieron su dinero y dañaron sus planes de vacaciones, negocios, etc...

Prevention

- 1. Usar sistemas de informacion actualizados, que apliquen politicas y restricciones que protegen y cuidan la informacion de gente con malas intenciones.
- 2. Tener a una persona encargada de constantemente examinar, analizar y proteger su red de datos.
- 3. Dar capacitaciones a los ususarios sobre lo importante que puede llegar a ser la seguridad de la informacion en una compañia que maneje muchos datos sencibles.