UIDE
Powered by
Arizona State University

Maestría en

CIBERSEGURIDAD

Tesis previa a la obtención del título de Magíster en Ciberseguridad

AUTOR:

- Ing. Denny Daniel Hidalgo Cedeño
- Ing. Luis Javier Ulloa Meneses
- Ing. Andrés Darío Villacís Valarezo

Auditoría de seguridad a la empresa Terminal Portuario de Manta

RESUMEN

En este trabajo, mediante una auditoría de ciberseguridad se explica el ataque sufrido por Hive Ransomware en la empresa vulnerando la red de servidores y generando caos de cara al cliente por la pérdida de información. La metodología de investigación utilizada en este documento es descriptiva cualitativa; porque se analiza la descripción de los fenómenos para conocer el origen de los eventos. Así mismo, se ha empleado una metodología híbrida de auditoría, apoyándose en las muchas ya existentes donde se desarrolla el análisis forense como base y un análisis de vulnerabilidades; ya que ambos terminan acoplándose a las casuísticas de la empresa. Entrando en contexto, se hizo un análisis de una imagen de disco duro y memoria RAM de un servidor afectado, con el propósito de encontrar evidencias relacionadas con el ataque sufrido. De la misma forma, se ejecutó un análisis de vulnerabilidades para hallar posibles brechas, amenazas y riesgos de ciberseguridad existentes para la empresa, tomando como punto de partida el estado de situación actual de la misma. Finalmente, se han reportado hallazgos respecto a la cadena de ataque del Ransomware, permitiendo desarrollar y aplicar estrategias y técnicas de mitigación que se han complementado con el análisis de vulnerabilidades donde se pudo obtener un snapshot de cómo está protegida la empresa a nivel de seguridad de la información; permitiéndonos realizar las recomendaciones pertinentes para minimizar el riesgo en pro de mejora continua y ciber resiliencia.

Palabras clave: Hive Ransomware, forense, vulnerabilidades, jboss, auditoria de ciberseguridad, tarea programada.

ABSTRACT

In this paper, by means of a cybersecurity audit, the attack suffered by Hive Ransomware in the company is explained, which violated the server network and generated chaos for the customer due to the loss of information. The research methodology used in this document is qualitative descriptive, because the description of the phenomena is analyzed to know the origin of the events. Likewise, a hybrid audit methodology has been used, relying on the many existing ones where the forensic analysis is developed as a basis and a vulnerabilities analysis, since both end up being coupled to the casuistry of the company. In context, an analysis of a hard disk image and RAM memory of an affected server was carried out in order to find evidence related to the attack suffered. In the same way, a vulnerabilities analysis was carried out to find possible gaps, threats and cybersecurity risks for the company, taking as a starting point the current situation of the company. Finally, findings regarding the Ransomware attack chain have been reported, allowing to develop and apply mitigation strategies and techniques that have been complemented with the vulnerabilities analysis where it was possible to obtain a snapshot of how the company is protected at the information security level, allowing us to make the relevant recommendations to minimize the risk in favor of continuous improvement and cyber resilience.

Keywords: Hive Ransomware, forensics, vulnerabilities, jboss, cybersecurity audit, scheduled task.