Resumen

El presente trabajo de titulación se enfoca en la implementación de un sistema de ciberseguridad destinado a reducir vulnerabilidades y posibles ataques del datacenter de FEMSA - Corporación GPF, que es una empresa consolidada en el Ecuador por más de 90 años enfocada en el retail farmacéutico y productos de conveniencia con más de 700 tiendas a nivel nacional por lo que es esencial salvaguardar la integridad, confidencialidad y disponibilidad de la información para una correcta operación de sus servicios.

El sistema de ciberseguridad está constituido con las consolas SaaS, Cloud One Workload Security y Vision One XDR de Trend Micro porque se someten a auditorías anuales para garantizar el cumplimiento de las mejores prácticas y siguiendo estándares de la industria como certificaciones ISO 27001, ISO 27014, ISO 27017, SOC2 y PCI DSS.

El proceso se divide en dos etapas: la implementación de las consolas y asignación de políticas de seguridad para cada servidor y configuración del sistema en los clientes seleccionados de alrededor de 400 servidores que conforman la infraestructura del data center. Estos clientes serán seleccionados mediante el análisis de su criticidad (alta, media o baja) basada en el sistema operativo, aplicación y ambiente de trabajo en el que se encuentra (Desarrollo, Test o Producción).

La etapa final consiste en la evaluación de la solución implementada que se pudo extraer que el índice de riesgo de los servidores ronda el 65%, que sería un punto de partida para mejorar la seguridad de estos, algunos de los sistemas operativos que están más expuestos son Microsoft Windows Server 2019 y 2016 como la distribución de Linux CentOS 7 los cuales requieren atención por presentar 1148 vulnerabilidades de seguridad conocidas. El retorno de la inversión obtenido en base al último reporte sobre el costo de un informe de violación de datos de IBM es del 3342% .

Palabras clave: Ciberseguridad, Trend Micro, Vulnerabilidades, Parcheo virtual

Abstract

This degree work focuses on the implementation of a cybersecurity system aimed at reducing vulnerabilities and possible attacks of the FEMSA datacenter - Corporation GPF, which is a consolidated company in Ecuador for more than 90 years focused on pharmaceutical retail and convenience products with more than 700 stores nationwide, so it is essential to safeguard integrity, Confidentiality and availability of information for the correct operation of its services.

The cybersecurity system is built on Trend Micro's SaaS, Cloud One Workload Security and Vision One XDR consoles because they undergo annual audits to ensure compliance with best practices and following industry standards such as ISO 27001, ISO 27014, ISO 27017, SOC2 and PCI DSS certifications.

The process is divided into two stages: the implementation of the consoles and assignment of security policies for each server and system configuration in the selected clients of around four hundred servers that make up the data center infrastructure. These clients will be selected by analyzing their criticality (high, medium, or low) based on the operating system, application, and work environment in which it is located (Development, Test or Production).

The final stage consists of the evaluation of the implemented solution that could be extracted that the risk index of the servers is around 65%, which would be a starting point to improve the security of these, some of the operating systems that are most exposed are Microsoft Windows Server 2019 and 2016 as the Linux distribution CentOS 7 which require attention for presenting 1148 known security vulnerabilities. The return on investment obtained based on the latest report on the cost of an IBM data breach report is 3342%.

Keywords: Cybersecurity, Trend Micro, Vulnerabilities, Virtual patching