CamWave
Comunicaciones Unificadas

Resumen Ejecutivo Conclusivo de la Consultoría.

SERVICIO DE CONSULTORÍA POR PRODUCTO PARA FORTALECIMIENTO Y MONITOREO DE LA INFRAESTRUCTURA TECNOLÓGICA – ELECCIONES SUBNACIONALES 2021

Entorno de Trabajo

Cliente	Órgano Electoral Plurinacional
Proyecto	CD-POE-R N° 127/2021 SERVICIO DE CONSULTORÍA POR PRODUCTO PARA FORTALECIMIENTO Y MONITOREO DE LA INFRAESTRUCTURA TECNOLÓGICA – ELECCIONES SUBNACIONALES 2021
Fecha	23 - Marzo - 2021

EthicalHacking Consultores

Índice

Antecedentes

Durante los días del 22 de febrero al 23 de marzo del año 2021, acorde al cumplimiento del contrato administrativo y los términos de referencia del **SERVICIO DE CONSULTORÍA POR PRODUCTO PARA FORTALECIMIENTO Y MONITOREO DE LA INFRAESTRUCTURA TECNOLÓGICA – ELECCIONES SUBNACIONALES 2021** para el proceso electoral de las Sub nacionales 2021 solicitado por el Órgano Electoral Plurinacional de Bolivia correspondiente al análisis y corrección de vulnerabilidades así como el fortalecimiento de las mismas.

Objetivos

- Realizar una análisis de intrusión interna, externa a la infraestructura de cómputo oficial.
- Apoyar con procedimientos de remediación las vulnerabilidades encontradas.
- Realizar un retest de las vulnerabilidades encontradas.
- Identificar y fortalecer las políticas y condiciones de seguridad de la infraestructura tecnológica.
- Realizar el monitoreo y seguimiento respectivo a los eventos suscitados en cada servidor con agente instalado.

Alcance de la consultoría

El alcance de la consultoría consiste en detectar posibles vulnerabilidades y la exposición de riesgo en la infraestructura tecnológica implementada por el OEP para la ejecución del proceso electoral subnacional 2021.

Este proceso deberá enmarcarse en la ejecución hacking ético a través de pruebas de intrusión externas e internas de tipo caja negra y/o caja gris, en un entorno asegurado y definido por el OEP, identificando la existencia de vulnerabilidades que pudiesen ser explotadas para comprometer la seguridad de los sistemas,hasta llegar a comprometer los distintos equipos de redes y comunicación, servidores, bases de datos y aplicaciones de la Institución a ser utilizados en el proceso electoral mencionado.

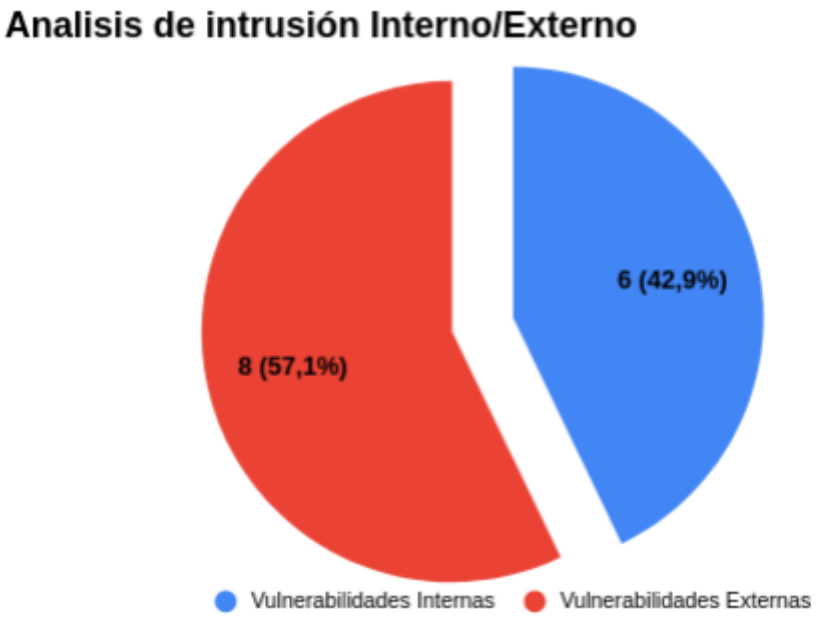
La consultoría abarca la siguiente infraestructura tecnológica:

- Servidores de cómputo oficial (red local para procesamiento y red en nube para publicación de resultados), mínimamente:
  - 12 controladores de dominio
  - 1 emisor de certificados
  - 2 servidor SCCM
  - 2 servidor antivirus
  - 1 servidor de monitoreo
  - 2 servidores de cómputo
  - 2 servidores de resultados
  - 10 servidores de imágenes

    - 2 servidores de publicación de servicios
- Bases de datos de cómputo
- Aplicación de escritorio de cómputo
- Aplicaciones web de resultados de cómputo
- Repositorio de imágenes
- Páginas Web de publicación de resultados de cómputo oficial
- Dispositivos de comunicación, firewalls y otros dispositivos que intervienen en el cómputo
- Aproximadamente 450 terminales de transcripción y verificación para proceso de cómputo
- Enlaces de comunicación entre TSE y Tribunales Departamentales.

Resumen

Las primera actividad a realizar fue análisis de intrusión externo y posteriormente el interno, en relación al análisis externo se encontró 6 vulnerabilidades y en relación al análisis interno se encontró 8 vulnerabilidades.



A continuación se realizó la tarea de corrección de las vulnerabilidades encontradas priorizando por criticidad y tiempo, estas vulnerabilidades priorizadas se llegaron a corregir todas.

Posteriormente se realizó la identificación de activos informáticos y se analizó su configuración, acorde a ello se brindó el apoyo para el fortalecimiento de la infraestructura tecnológica.

Finalmente se procedió a monitorizar todos los eventos durante el proceso electoral, la recolección de eventos se realizó mediante el uso de agentes los cuales recolectan

información de los logs y eventos del servidor para posteriormente hacer el análisis con dicha información.

Resultados

Durante todo el proceso de la consultoría brindada se pudieron evidenciar los siguientes puntos:

- Se creó un documento con las vulnerabilidades internas y externas que se encontraron.
- Se realizó la Re-evaluación de cada vulnerabilidad y se encontró que todas las vulnerabilidades priorizadas fueron mitigadas.
- No hubo tráfico irregular o sospechoso detectado en los equipos de seguridad perimetral. Todo tráfico identificado durante el monitoreo fue respaldado y verificado con el personal a cargo de OEP.
- Se presentó un documento con la identificación y fortalecimiento de la infraestructura tecnológica.
- Se identificaron cortes de energía eléctrica durante el proceso de elección en TED La Paz, Chuquisaca y Tarija, sin embargo, se resolvió de manera oportuna por el personal de OEP y no se suscitaron problemas mayores.

Conclusiones

Se puede concluir lo siguiente:

- Se encontraron vulnerabilidades externas e internas, de las cuales los más críticos para el proceso de cómputo fueron mitigadas en etapas tempranas.
- El apoyo en el fortalecimiento de la infraestructura tecnológica fue satisfactorio.
- Durante el proceso de monitoreo se detectaron eventos que fueron debidamente aclarados y respaldados en su momento, asimismo ninguno afectó a la integridad de los datos a lo largo del proceso de cómputo de las Elecciones Subnacionales 2021.

Alejandro Mario Orias Rodriguez
Gerente General
Camwave S.R.L.