SERVICIOS DE CIBERSEGURIDAD

CLIENTE: ORGANO ELECTORAL PLURINACIONAL

REFERENCIA: INFORME FINAL Y CONCLUSIVO

Fecha: DICIEMBRE, 2024

INFORME FINAL

Índice

INFORME DE ANÁLISIS DE SEGURIDAD DE LOS SISTEMAS INFORMÁTICOS PARA LAS ELECCIONES JUDICIALES 2024

Entre los días 28 de octubre y 14 de diciembre de 2024, el equipo consultor de 4SECURITY LATAM llevó a cabo las pruebas correspondientes al Análisis de Seguridad de los Sistemas Informáticos en el marco de las Elecciones Judiciales 2024. Este trabajo fue solicitado por el Órgano Electoral Plurinacional (OEP) con el objetivo de realizar una evaluación integral de la seguridad de la plataforma informática y de los controles de seguridad implementados para garantizar la protección de la información.

De manera paralela, y hasta el 18 de diciembre de 2024, el equipo consultor de 4SECURITY LATAM brindó acompañamiento en la corrección de vulnerabilidades y en la reevaluación de los hallazgos identificados sobre los activos clasificados como prioritarios. Posteriormente, se procedió con la corrección de los elementos asociados a riesgos críticos y altos.

El análisis de seguridad comprendió la ejecución de dos actividades principales:

1. Pruebas de penetración externas.
2. Pruebas de penetración internas.

Todas las pruebas fueron realizadas bajo la modalidad de caja negra (sin conocimiento previo de los elementos a analizar) y caja gris, en cuyo marco se proporcionó conectividad a la red interna y acceso a cuentas de usuario en los aplicativos de dicha red. Como resultado, se identificaron observaciones con diferentes niveles de criticidad.

EVALUACIÓN EXTERNA

La evaluación externa permitió identificar vulnerabilidades en los servicios expuestos a internet bajo los subdominios del OEP (*.oep.org.bo). La entidad solicitó priorizar los hallazgos relacionados con los servidores de plataformaciudadanos.oep.org.bo y de cómputo, los cuales fueron empleados durante la publicación de los resultados de las elecciones judiciales 2024. Estos hallazgos priorizados fueron mitigados satisfactoriamente.

EVALUACIÓN INTERNA

Durante la evaluación de la infraestructura interna se constató que el OEP había implementado una red independiente de la red de trabajo habitual del personal interno. Esta red se encontraba aislada de la conectividad a internet y fue empleada para el cómputo de los resultados electorales. Entre los controles de seguridad implementados en dicha red se destacaron:

- Un gestor de configuraciones y parches de seguridad.
- Mecanismos de segregación de la red interna.
- Antivirus instalado en equipos con sistema operativo Windows.
- Sistemas de monitoreo activos.

EVALUACIÓN DE APLICATIVOS

El análisis incluyó la revisión de:

- Aplicativos de escritorio para el procesamiento de actas (SCORC).
- Aplicativos web para la presentación de resultados (computo.oep.org.bo) tanto en su versión interna (preproducción) como en la publicada en internet.

CONCLUSIONES

Se concluye que, tras las mitigaciones realizadas y las medidas de seguridad implementadas en el Órgano Electoral Plurinacional (OEP), se ha establecido un entorno de seguridad confiable. Estas medidas incluyen:

- Control de acceso físico: Restricción estricta para el ingreso a las instalaciones donde se encuentra la infraestructura crítica.
- Habilitación manual del acceso a la red de cómputo: Implementación de un proceso manual y supervisado para autorizar conexiones a la red de cómputo.
- Acceso físico restringido a los equipos de cómputo: Limitación del acceso directo a los equipos utilizados en el procesamiento y cómputo de resultados.
- Cifrado de discos: Protección de la información almacenada mediante la implementación de sistemas de cifrado en los discos duros.
- Agente antivirus y equipo de monitoreo: Uso de soluciones antivirus actualizadas en los equipos, complementadas con un equipo de monitoreo dedicado para la supervisión constante del comportamiento de la red y la detección de posibles anomalías o incidentes de seguridad.
- Uso de cuentas de usuarios con bajos privilegios: Restricción de permisos durante el proceso de transcripción para minimizar los riesgos asociados a accesos no autorizados o ejecución de acciones críticas.

Estas acciones han sido clave para garantizar un entorno de seguridad de alto nivel, dificultando significativamente la posibilidad de accesos no autorizados tanto en la red interna como en los equipos críticos. El conjunto de controles implementados refleja un compromiso con la protección de la información y la mitigación de riesgos asociados al proceso electoral.


4SEC
Your Technological Ally With Strategic Thinking