Informe de Auditoria IEEH 2018 UNAM FES Acatlán Publicación

Elección 2018, diputaciones locales

HIDALGO
IEE
INSTITUTO ESTATAL ELECTORAL

FES UNAM ACATLÁN

Facultad de Estudios Superiores
Acatlán

Junio de 2018

Contenido

Presentación

De acuerdo con la Ley General de Instituciones y Procedimientos Electorales (2017), el Programa de Resultados Electorales Preliminares (PREP) "es el mecanismo de información electoral encargado de proveer los resultados preliminares, de carácter estrictamente informativo y no definitivos, de las elecciones" (pág. 99). Uno de los elementos medulares del PREP es el sistema informático que emplea para la digitalización de las actas de escrutinio y cómputo, así como para la captura, verificación y publicación de esta información vía Internet.

Según el tipo de elecciones que se trate, la responsabilidad de implementar y operar cada instancia del PREP recae en el Instituto Nacional Electoral (INE) o bien en alguno de los 32 Organismos Públicos Locales (OPL) del país.

Los Lineamientos del PREP (2017) señalan que el INE o los OPL deben someter su sistema informático a una auditoría de verificación y análisis, "con la finalidad de evaluar la integridad, disponibilidad y seguridad en el procesamiento de la información y la generación de resultados conforme a la normativa aplicable y vigente" (pág. 3), para lo cual deben designar un ente auditor. De acuerdo con el artículo 347 del Reglamento de Elecciones (INE, 2016), "para la designación del ente auditor se dará prioridad a instituciones académicas o de investigación" (pág. 232).

A partir de lo anterior, el Instituto Estatal Electoral de Hidalgo (IEEH), en su calidad de OPL, designa como ente auditor de la aplicación informática del PREP a la FES Acatlán de la Universidad Nacional Autónoma de México (UNAM), de cara a las elecciones 30 diputaciones locales, a realizarse el primero de julio de 2018.

Plan de pruebas

1. Pruebas funcionales de caja negra al sistema informático del PREP para evaluar la integridad en el procesamiento de la información: digitalización (obtención de la imagen digital del acta), captura (de actas PREP), validación (de la información capturada), generación y publicación de resultados preliminares (emisión de reportes y despliegue, de conformidad con la normatividad aplicable).
   Para este efecto, la FES Acatlán estimo los resultados de todas las casillas proyectadas para la jornada electoral del 1 de julio de 2018 (diputaciones locales) y, con apoyo del IEEH, instrumento y observo el desarrollo de un simulacro especial de auditoría, en donde se puso a prueba la aplicación informática del PREP, al cotejar sus resultados con los estimados por la FES Acatlán. Durante el citado simulacro, la FES Acatlán observo directamente el desarrollo de los trabajos, tanto en el Centro de Cómputo Estatal, como en algunos de Centros de Acopio y Transmisión de Datos.

2. Análisis de vulnerabilidades, considerando pruebas de penetración y revisión a las configuraciones de seguridad de la infraestructura tecnológica del PREP.
   Las pruebas de penetración (*pentest*) consistieron en la ejecución de herramientas informáticas para identificar potenciales vulnerabilidades, desde dentro y fuera de la red de

datos, particularmente en servidores, aplicaciones web, equipos de telecomunicaciones y estaciones de trabajo. Posteriormente se aplicarán diversas técnicas para intentar explotar las vulnerabilidades detectadas.

3. Revisión de configuraciones de seguridad de la infraestructura tecnológica del PREP. Consistirá en la evaluación de los sistemas operativos de los dispositivos que conforman la infraestructura tecnológica del PREP, a través de la comparación con buenas prácticas internacionales de seguridad informática.

4. Pruebas de negación del servicio al sitio web de PREP y al sitio principal del IEEH.
   Dichas pruebas involucrarán la generación de tráfico de red no malintencionado y malintencionado, tanto desde fuera como dentro de la red de datos del IEEH, y ataques en la capa de aplicación HTTP.

5. Se realizó el procedimiento técnico para validar el software y la base de datos del PREP. Esencialmente se trata de validar que el sistema informático del PREP que operará el día de la jornada electoral, corresponda al software auditado, se realizó la a generación de huellas criptográficas en SHA-256 del software PREP.

Se rinde la presente a nuestro leal saber y entender.

28 de junio de 2018

Resultados pruebas de caja negra

El presente documento presenta los resultados de las pruebas de caja negra realizadas durante la prueba de auditoria al Programa de Resultados Electorales Preliminares del Estado de Hidalgo.

Generación de datos de prueba

La Unidad Técnica de Informática proporcionó a la FES Acatlán, a través del Ing. Said Rodríguez García, una base de datos con cantidades muestra para el llenado de actas de cada uno de los distritos del Estado de Hidalgo.

A su vez, la FES Acatlán generó cantidades aleatorias para modificar los archivos y los regresó a la Unidad Técnica de Informática para que ellos a su vez organizaran el llenado y distribución de las actas de prueba.

Validación

Una vez realizado el simulacro especial, se le proporcionó a la FES Acatlán los datos de los resultados en un archivo de texto separados por pipes (|):

[redacted].rpt

Utilizando un proceso automático, se cotejó dato a dato para encontrar diferencias entre lo que aparecía en el acta y lo que se capturó en el sistema. Los resultados de la comparación se detallan en el archivo:

[redacted].xlsx

El archivo contiene los datos obtenidos en la prueba y los datos generados por la FES Acatlán, una hoja por cada Distrito. Las diferencias se marcaron y se agregó un comentario a la celda con el dato que se capturó.

Resultados

En el simulacro se encontraron los siguientes casos, tomando como base los datos que la FES Acatlán proporcionó a la Unidad Técnica de Informática:

1. **Errores al transcribir los datos de la FESA en las actas**. Dado que se trató de un proceso manual, algunos de los datos fueron escritos de forma incorrecta en las actas de papel.
2. **Errores de uno o varios datos capturados en el sistema**. La validación automática señala que hay diferencias, pero éstas se deben a un error de captura (factor humano no mal intencionado).
3. **Actas cuya captura de datos e imagen escaneada fueron intercambiadas**. Como parte de los errores de transcripción, algunas actas fueron llenadas con los datos de otra y en ocasiones fueron intercambiadas.

4. **Algunas actas están marcadas con la leyenda "Ilegible"**. En efecto, los datos no son legibles en la mayoría de las actas escaneadas que presentan esta leyenda.

5. Cabe señalar que casos que revisamos, escaneados con celular, si son ilegibles.

Se concluye que las diferencias encontradas en los puntos 1, 2 y 3 se debieron al uso de datos diferentes a los proporcionados por la FES Acatlán o por errores de captura, pero no son atribuibles al aplicativo PREP.

El punto 5 requiere de una revisión para evitar que se publiquen datos que causen confusión. Se recomienda que se le haga énfasis al responsable de tomar las fotografías sobre la importancia de la calidad de la misma.

Pruebas de penetración

1. Se realizó el servicio de pruebas de penetración a la infraestructura de los activos designados por el IEEH durante un simulacro, para la explotación de posibles brechas de seguridad que permitieran el acceso no autorizado en los sistemas o aplicativos.
2. Acorde con el esfuerzo requerido para llevar a cabo la explotación de las vulnerabilidades identificadas y de acuerdo con las mejores prácticas, se considera un nivel de riesgo Alto sobre los activos evaluados ya que múltiples activos carecen del parche de seguridad [redacted] catalogado como crítico por el fabricante.
3. Un usuario mal intencionado podría explotar esta vulnerabilidad y extraer información sensible del Instituto de forma remota, debido a que esta vulnerabilidad puede explotarse de forma remota y sin la necesidad de credenciales.
4. Durante las pruebas de penetración a la infraestructura del IEEH se identificó que la red del Instituto cuenta con la debida segmentación y controles de acceso entre redes y recursos.
5. Se identifica el uso del protocolo por [redacted] en su versión 1, se recomienda el cese al uso de este protocolo debido a sus múltiples vulnerabilidades presentes comparados a otros protocolos de comunicación.
6. Es necesaria la reconfiguración de los algoritmos robustos para el uso del protocolo de comunicación SSH.
7. Se identifica la ausencia de certificados digitales en los aplicativos web de: www.ieehidalgo.org.mx y [redacted], la comunicación entre el cliente y el servidor no se encuentra cifrada, un atacante podría interceptar el tráfico entre el cliente y el servidor y hacer un robo de información sensible. Asimismo se identifica configuraciones deficientes para los directorios y activos que lo componen permitiendo la enumeración y acceso a diversos recursos del sitio.
8. En el portal www.ieehidalgo.org.mx se identifica una versión vulnerable de Apache que cuenta con una brecha de seguridad, al ser explotada podría dar como resultado una denegación de servicio en el activo.
9. En el portal alojado en la IP pública [redacted] se identifica la presencia de un repositorio [redacted] y los archivos que lo componen, un usuario mal intencionado podría comprometer el sitio.

10. Se identifica la ausencia de múltiples parches de seguridad para diversos activos, es importante seguir las recomendaciones del fabricante para mantener los activos seguros.

Pruebas de negación de servicio

Se realizó un ataque de denegación de servicio por medio de SYN FLOOD con la intención de validar los controles de seguridad implementados para la protección del activo. Se identifica que los paquetes comienzan a ser rechazados por los controles de seguridad por parte del proveedor del servicio de hosting. Si bien el acceso al recurso puede ser un poco lento, **su funcionalidad no es afectada**.

Conclusiones

Reconocemos el esfuerzo que el Instituto ha realizado respecto al PREP y percibimos un proceso diferente con respecto a otros ejercicios ya realizados con esta institución, debido esto al Reglamento de Elecciones en su Artículo 347 emitidos por el INE que en búsqueda de esa certeza y confiabilidad agrega nuevos procesos como la digitalización y presentación de las Actas de Escrutinio y Cómputo más la captura por medio de teléfonos móviles.

Como resultado de la auditoria se concluye que el sistema informático del Programa de Resultados Electorales Preliminares (PREP) desarrollado por el Instituto Electoral del Estado de Hidalgo, cumple con las medidas que permiten, la confidencialidad, la integridad y la disponibilidad adecuada pertinente para el apoyo en la digitalización, captura y publicación vía internet de la información asentada en las actas de escrutinio y cómputo. La información es procesada de manera adecuada y los resultados preliminares son publicados conforme es requerido.

Indiscutiblemente hay área de oportunidad derivado esto del origen de la información como en todo sistema informático. La calidad y funcionalidad de los datos depende de sus entradas, que en el caso tienen origen en las actas de escrutinio y cómputo llenadas en las diversas casillas asentadas en el estado por los ciudadanos insaculados para tal efecto, por lo cual será importante el recordar a los funcionarios y potenciar acciones orientadas al adecuado llenado de dichas actas.

Nuestras conclusiones-recomendaciones relativas a las vulnerabilidades y riesgos detectados son las siguientes:

1. Se debe tener un proceso efectivo de planeación para el análisis, diseño, construcción y pruebas del sistema informático del PREP, con hitos bien definidos que permitan que las etapas administrativas y jurídicas del proceso electoral culminen con la anticipación adecuada para instrumentar, bajo principios de aseguramiento de la calidad de software, los cambios y adiciones en el código de la aplicación.

2. Actualizar el software publicador Web. Asimismo, instrumentar un procedimiento riguroso de actualización de versiones de sistema operativo, base de datos y publicador de servicios web.

3. Gestionar y preferentemente utilizar certificados emitidos por entidades reconocidas y desestimar el uso de certificados autofirmados.

4. Desestimar el uso de servicios de control de versiones en servidores en producción.

5. Reforzar el procedimiento de capacitación al personal de los CATD's y de la Sede Central.

6. Considerar la pertinencia de gestionar en al ámbito de su propia competencia, las adecuaciones pertinentes que faciliten la instrumentación eficaz del PREP y contribuyan a fortalecer sus características esenciales de integridad, exactitud, confiabilidad y seguridad, en estricto apego a los Lineamientos del Programa de Resultados Electorales Preliminares.

-*-