INFORME AUDITORIA DE PKI A ENTIDAD DE CERTIFICACION AVANSI S.R.L. 2020

DIRECCIÓN DE CIBERSEGURIDAD, COMERCIO ELECTRONICO Y FIRMA DIGITAL

12/03/2020

Equipo de Auditores
Ing. José Raúl Madera Oropeza
Lic. Richard N. Sarmiento Rosario

Introducción

Según el Artículo 56 de la Ley Núm. 126-02 sobre Comercio Electrónico, Documento y Firmas Digital, el INDOTEL podrá realizar auditorías ordinarias anuales para asegurar el correcto funcionamiento y la eficiente prestación del servicio de certificación digital a las Entidades de Certificación (CA) del país. En este caso, procedemos a la auditoria anual correspondiente al 2020 de AVANSI, S.R.L. (España) autorizada a operar como Entidad de Certificación (CA), mediante la Resolución del Consejo Directivo Núm. 166-06 de fecha 28 de septiembre de 2006.

Base de los resultados

La presente auditoria se realizó basándonos en la Norma complementaria por la que se establece la equivalencia regulatoria del sistema Dominicano de Infraestructuras de Clave Publicas y de confianza con los marcos regulatorios Internacionales de servicios de confianza. ETSI EN 319 401 Norma de requisitos de política general para proveedores de servicios de confianza, esta normas es un requisito para los organismos de evaluación de la conformidad que evalúan proveedores de servicios de confianza y la Norma ETSI EN 319 411-1 son los requisitos de políticas y seguridad para los proveedores de servicios de confianza que emiten certificados. La misma nos muestra una compilación de recomendaciones para las prácticas exitosas de seguridad que toda organización puede aplicar independientemente de su tamaño o sector. Las normas técnicas fueron redactada intencionalmente para que fuera flexible y nunca indujo a las personas que la cumplían para que prefirieran una solución de seguridad específica. Las recomendaciones de la norma técnica ETSI EN 319 401 y ETSI EN 319 411-1 son de forma Neutrales.

Alcance

Esta auditoria incluye todos los controles específicos sobre Infraestructura de Clave Pública (PKI) que comprenden los temas de seguridad informática, seguridad de la información, controles criptográficos y ciclo de vida de los Certificados Digitales, según la normativa vigente en la República Dominicana para las Entidades de Certificaciones.

Plan de Auditoria

Fecha/Hora	Auditor	Área/Función proceso/Actividad	Auditado	Lugar
12-3-2020 9:00am,9:15am	Jose Raul Madera Richard Sarmiento	Llegada a la Organización	N/A	Oficina Principal Santo Domingo
12/3/2020 9:30am,10:00am	Jose Raul Madera Richard Sarmiento	Reunión de Apertura	Encargado de Area	Oficina Principal Santo Domingo
12-3-2020 10:00am,11:00am	Jose Raul Madera Richard Sarmiento	Análisis Documental	Registrador	Oficina Principal Santo Domingo
12-3-2020 11:00am,12:00am	Jose Raul Madera Richard Sarmiento	Prueba y Análisis Vulnerabilidades Interna y externa	Encargado de Unidad de registro	Oficina Principal Santo Domingo
12-3-2020 12:00am,12:30am	Jose Raul Madera Richard Sarmiento	Almuerzo	N/A	Oficina Principal Santo Domingo
12-3-2020 12:40am,1:00pm	Jose Raul Madera Richard Sarmiento	Análisis Vulnerabilidades del Website de la CA	Encargado de la RA, Registrador	Oficina Principal Santo Domingo
12-3-2020 1:00pm,2:00pm	Jose Raul Madera Richard Sarmiento	Reunion de Cierre	Encargado de la RA	Oficina Principal Santo Domingo

Participantes Reunión de Apertura

Carlos David Gómez
José Raúl Madera Oropeza
Richard N. Sarmiento Rosario

Participantes Reunión de Cierre

Carlos David Gómez
José Raúl Madera Oropeza
Richard N. Sarmiento Rosario

Lista de Personal Entrevistado

Carlos David Gomez

Resumen de la auditoría

En fecha 12 de marzo de 2020, en las instalaciones de AVANSI, S.R.L., sito en la Av. Lope de Vega, No. 19, Edificio PIISA A, Suite 102, 1ra. Plt. Ensanche Naco, Santo Domingo República Dominicana, se inició el proceso de verificación documental sobre Manual de Procedimiento, Planes de Contingencia, Continuidad de Negocio, Cese de Actividades, contratos con terceros sobre Infraestructuras como servicio y servicios de colocación, además de las Políticas de Seguridad y Protección de Datos. En ese sentido, se procedió a analizar dicha información documentada con respecto a los criterios exigidos en las Normas Complementarias sobre Procedimientos de Seguridad, Estándares Tecnológicos, Protección de Datos, Políticas y Procedimientos de Certificación, entre otros.

Se verificó el entorno físico operativo que sirve como recepción de suscriptores para los procesos de acreditación y emisión de Certificados Digitales y el ambiente físico operativo de AVANSI, SRL. Se entrevistó al señor Carlos David Gómez, responsable del manejo de la PKI.

Se revisaron los componentes y controles técnicos requeridos por la normativa vigente de acuerdo a los temas sobre la Política de Seguridad Institucional, Organización de la Seguridad, Clasificación y Control de Activos, Seguridad del Personal, Seguridad Física y Ambiental, Gestión de Comunicaciones y Operaciones, Control de Accesos, Desarrollo y Mantenimiento de Sistemas, Administración de la Continuidad del Negocio, puntualizando las revisiones en las áreas de TI, Gestión Humana, Operaciones y Seguridad Física de la empresa.

En adición a lo anterior, se ejecutó la herramienta de análisis de vulnerabilidades al módulo de registro web, llamada Owasp-zap, el cual descubrió la existencia de doce (12) vulnerabilidades catalogadas de alto, medio y bajo impacto, las cuales se detallan en este informe.

Sumario de Hallazgo y Observaciones

En esta auditoría de seguimiento se procedió a la verificación documental y se pudo observar que los hallazgos encontrados en la auditoria anterior, referente a la política de seguridad de AVANSI que se había establecido que los mismos carecían de un orden cronológico tal cual lo dicta nuestra normativa, la Entidad de Certificación procedió a realizar los cambios y adaptaciones necesaria y de esta manera solucionaron en su totalidad dichos hallazgos. Como medida de garantizar una mejor Protección de los Datos y a la vez eficientizar la seguridad de la PKI, nos informaron que tienen agendado para el próximo año el traslado de los Servidores de la Infraestructura de Clave Pública (PKI) que se encuentran en Barcelona España hasta Sevilla.

En cuanto a los planes de continuidad del negocio se pudo comprobar que en fecha 13-9-2019 y el 7-11-2019, se procedió a la activación del plan de contingencia con la finalidad de realizar varias pruebas que consistían en eliminar las claves de la PKI, formateo del HSM, inicialización del mismo y restauración de las copias de las llaves, con el fin de simular un caso de fallo crítico y la segunda prueba que se realizo fue de la pérdida de sincronización del reloj en TSU y de estas Pruebas arrojaron una serie de errores y en su defecto se procedió a corregirla. Las operaciones de la Entidad de Certificación no se evidenciaron ningún tipo

de cese de actividad y todos sus controles se encuentran operando de manera satisfactorios, los contratos con tercero sobre servicio de Infraestructuras y servicio de colocación se pudo establecer que se encuentran actualizados.

Cabe destacar que los hallazgos y las observaciones que se evidenciaron en el informe final de la auditoría del 2019 de la Entidad de Certificación de AVANSI, fueron corregidos en su totalidad y a la fecha todos sus documentos se encuentran en orden y en afinidad con nuestra normativa jurídica.

En adición se ejecutó la herramienta de análisis de vulnerabilidades web, al módulo de registro, llamada Owasp-zap, el cual descubrió la existencia de doce (12) vulnerabilidades catalogada de alto, medio y bajo impacto, las mismas se detallan en este informe.

Alertas encontradas en el análisis de vulnerabilidad del sitio web:

Summary of Alerts

Risk Level	Number of Alerts
High	2
Medium	4
Low	6

Nivel de alerta: Alto
ID de alerta: Falla por Inyección SQL
Descripción: Se comprobó que una inyección por SQL puede ser posible.

Nivel de alerta: Alto
ID de alerta: Recorrido del directorio
Descripción: La técnica de ataque Path Traversal permite a un atacante acceder a los archivos, directorios y comandos que potencialmente residen fuera del directorio raíz de documentos web. Un atacante puede controlar una URL de tal forma que el sitio web ejecutará o mostrará la información de los archivos que son arbitrarios en cualquier parte del servidor web. Cualquier dispositivo que se exponga a una interfaz que se basa en HTTP es potencialmente vulnerable a un Path Traversal. La mayoría de los sitios web prohíbe el acceso de los usuarios a algún sitio específico del sistema de los archivos, normalmente denominado directorio "raíz del documento web" o "raíz CGI". Estos directorios poseen los archivos que están destinados al acceso del usuario y el ejecutable que es necesario para poder controlar la funcionalidad correcta de la aplicación web. Para poder ingresar a los archivos o activar los comandos en cualquier zona del sistema de los archivos, los ataques de trayectoria de rutas van a utilizar la capacidad de las secuencias de todos los caracteres especiales. El ataque Path Traversal más elemental utiliza la secuencia de los caracteres especiales "../" para poder modificar la ubicación del recurso que es requerido en la URL. Aunque la gran mayoría de los servidores web que son populares van a evitar que esta técnica se escape de la raíz del documento web, las codificaciones que son alternativas de la secuencia "../" pueden impedir los filtros de seguridad. Inclusive si el servidor web impide de forma correcta los intentos de trayectoria en la ruta de la URL, una aplicación web en sí misma puede ser muy vulnerable provocado por el manejo de

forma incorrecta de la entrada que fue proporcionada por el usuario. Este es un problema muy común de las aplicaciones web que utilizan los mecanismos de plantilla o cargan algún texto estático de los archivos. En las variaciones de los ataques, el valor del parámetro de la URL original se modifica por el nombre de uno de los archivos de órdenes dinámicos de la aplicación web. Provocando que, los resultados puedan mostrar el código fuente porque el archivo se interpreta como un texto en vez de como un archivo de órdenes ejecutable. Estás técnicas muchas veces utilizan caracteres especiales extras, como el punto (".") para poder revelar la lista del directorio de trabajo actual, o los caracteres que son NULOS "%00 para poder evadir las verificaciones elementales de la extensión de los archivos.

Nivel de alerta: Medio/alto

ID de alerta: ID de sesión en reescritura de la URL

Descripción: La reescritura de la URL se utiliza para rastrear la ID de sesión del usuario la ID de la sesión puede divulgarse a través del encabezado de referencia del sitio cruzado. Además, la ID de la sesión puede almacenarse en el historial del navegador o en los registro del servidor.

Nivel de alerta: Medio

ID de alerta: El encabezado X-Frame-Options no está establecido

Descripción: El encabezado X-Frame_Options no se encuentra incluido en la respuesta HTTP para la protección ante los ataques secuestro de clic o ataque de compensación de UI (ClickJacking).

Nivel de alerta: Medio

ID de alerta: Referer expone ID de sesión

Descripción: Se encontró un hipervínculo que apunta a otro nombre de host. A medida que se utiliza la reescritura de URL de ID de sesión, puede divulgarse en el encabezado de referencia a hosts externos.

Nivel de alerta: Medio

ID de alerta: Error de formato de cadena

Descripción: Un error de formato de cadena ocurre cuando los datos de una cadena de entrada es evaluada como un comando por la aplicación.

Nivel de alerta: Bajo

ID de alerta: Incompleto o no Cache-control y sistema de encabezado HTTP Pragma.

Descripción: El cache-control y encabezado HTTP Pragma no ha sido establecido apropiadamente o faltan, permitiendo al navegador y servidores proxy almacenar contenido.

Nivel de alerta: Bajo

ID de alerta: El servidor pierde información a través de los campos de encabezado de respuesta HTTP "X_PoweredBy"

Descripción: El servidor web / de aplicaciones está filtrando información a través de uno o más encabezados de respuesta HTTP "X-Powered-By". El acceso a dicha información puede facilitar a los atacantes identificar otros marcos / componentes de los que depende su aplicación web y las vulnerabilidades a las que pueden estar sujetos dichos componentes.

Nivel de alerta: Bajo

ID de alerta: Ausencia de tokens anti-CSRF

Descripción: No se encontraron tokens Anti-CSRF en un formulario de envío HTML. Una solicitud falsa entre sitios en un ataque que compromete y obliga a una víctima a enviar su solicitud HTTP a un destino objetivo sin su conocimiento o intención para poder realizar una acción como víctima. La causa oculta es la funcionalidad de la aplicación utilizando acciones de URL/formulario que pueden ser adivinados de forma repetible. La naturaleza del ataque es que CSRG explota la confianza que un sitio web proporciona a un usuario. Por el contrario, las cadenas de comandos de los sitios cruzados (XSS) explotan la confianza que un usuario proporciona en un sitio web. Al igual que XSS, los ataques CSRG no son de forma necesaria de sitios cruzados, pero hay la posibilidad de que si pueden serlo. La falsificación de las solicitudes ante los sitios también se conoce como CSRF, XSRG, ataques con un solo clic, montaje de sesión, diputado confundido y navegación en alta mar.
Los ataques de CSRG son muy efectivos en varias situaciones, que incluyen:
*La victima tiene una sesión activa en el sitio de destino.
*La víctima se autoriza por medio de la autenticación HTTP en el sitio de destino.
*La víctima se encuentra en la misma red local que el sitio de destino.
CSRF se ha utilizado especialmente para poder realizar una acción contra un sitio objetivo utilizando los privilegios de la víctima, pero se han revelado técnicas recientes para difundir información al obtener el acceso a la respuesta. El riesgo de divulgación de información aumenta de forma drástica cuando el sitio de destino se encuentra vulnerable a XSS, porque XSS se puede utilizar como una plataforma para CSRF, lo que le permite al atacante que opere desde adentro de los límites de la misma política de origen.

Nivel de alerta: Bajo

ID de alerta: Una cookie sin el atributo SameSite.

Descripción: Se ha establecido una cookie sin el atributo SameSite, lo que significa que la cookie se puede enviar como resultado de una solicitud "entre sitios". El atributo SameSite es una contramedida efectiva para la falsificación de solicitudes entre sitios, la inclusión de scripts entre sitios y ataques de tiempo.

Nivel de alerta: Bajo

ID de alerta: Divulgación de error de aplicación

Descripción: Esta página contiene un mensaje de error/advertencia que podría revelar información sensible como la ubicación del archivo que produjo la excepción no controlada. Esta información puede ser usada para lanzar futuros ataques contra la aplicación web. La alerta podría ser un falso positivo si el mensaje de error es encontrado dentro de una página de documentación.

Nivel de alerta: Bajo

ID de alerta: Cookie sin bandera asegurada

Descripción: Una cookie ha sido enviada sin la bandera asegurada, lo que significa que la cookie puede ser accedida mediante conexiones sin cifrar.

Recomendaciones y soluciones a las vulnerabilidades:

1. **Fallas por inyección SQL:** No confié en los valores de entrada del lado del cliente, incluso si en el lado del cliente se realice una validación. En general, compruebe todos los datos de entrada en el servidor, en caso de que la aplicación usa JDBC, le recomiendo usar PreparedStatement o CallableStatement, con los parámetros

pasados por "?". Otra solución en caso que la aplicación utiliza ASP, se recomienda usar ADO Conmand Objects con una fuerte comprobación de tipos de consultas y parámetros. En el caso de que la base de datos pueda usar Stored Procedures o procedimientos de almacenamientos úselo. No concatene cadenas en los query o consultas, en el procedimiento almacenado o utilizar exec inmediate o su funcionalidad equivalente. No crear consulta SQL dinámica usando cadena sencilla de concatenación. Aplique a una lista blanca de carácter permitido o una lista negra de carácter no permitido en la entrada del usuario. Aplicar el privilegio mínimo posible al o los usuarios de la base de datos de los privilegios usados. En lo particular evitar el uso de los usuarios de base de datos "sa" o "db-owner", esto no elimina la inyección SQL, pero minimiza su impacto.

2. **Ataque Paht Traversal (Directory Traversal):** asuma que todas las entradas son maliciosa, utilice una estrategia de validación de entrada, es decir, utilice alguna lista blanca de entradas aceptadable que se ajuste de estricta a las especificaciones o cámbiela por algo que en realidad lo realice, no confié solamente en la búsqueda de entradas maliciosa o mal formada (no confié en lista negra). Sin embargo, las listas negras pueden ser muy útiles para detectar posibles ataques o diagnosticar cuales entradas están más formadas que se deberían rechazar directamente. Al realizar la validación de entrada, usted debe considerar todas las propiedades potencialmente destacadas, incluida la longitud, el tipo de entrada, el rango completo de valores aceptables, las entradas faltantes o adicionales, la sintaxis, el sentido entre los campos que se encuentran relacionados y la conformidad con todas las reglas comerciales. Como un ejemplo de lógica de las reglas comerciales, "bote" puede ser válido de forma sintáctica porque solo posee caracteres que son alfanuméricos, pero no es válido si está esperando los colores como "rojo" o "azul". Para los nombres de los archivos, utilice las listas blancas que son estrictas y que limiten el grupo de caracteres que se van a utilizar. Si es posible, solo permita un solo carácter "." en el nombre del archivo para poder prevenir las vulnerabilidades y rechazar los separadores de directorios como por ejemplo "/". Utilice una lista blanca de las extensiones del archivo que sea permitida. Advertencia: si usted intenta limpiar sus datos, tiene que hacerlo para que el resultado final no esté en la forma en el que estos puedan ser un peligro. Un mecanismo para desinfectar puede provocar la eliminación de caracteres como por ejemplo "." y ";" que pueden ser necesitados para varias explosiones. Un atacante puede intentar burlar al mecanismo de desinfección para que este "limpie" los datos de una forma que puede ser muy peligrosa. Supongamos que el atacante logra inyectar un "." dentro de un nombre de un archivo (por ejemplo, "archivo sensi.tive") y el mecanismo que se encarga de desinfectar elimina el carácter que da como resultado que el nombre del archivo válido sea, "archivo sensible". Si ahora suponemos que los datos de entrada son seguros, entonces el archivo tiene la posibilidad de verse comprometido.

3. **ID de sesión en reescritura de URL:** Para contenido seguro, coloque la Id de sesión en una cookie. Para estar aún más seguro, considere usar una combinación de cookies y reescritura de URL.

4. **Encabezado X-Frame-Option no se encuentra establecido:** Los navegadores web más modernos apoyan el encabezado HTTP X-Frame-Options. Asegúrese que está establecido en todas las páginas web devuelta por su sitio (si usted espera que la pagina este enmarcada solo por página en su servidor, ejemplo, es parte de un FRAMESET, entonces usted querrá usar SAMEORIGIN, de ALLOW-FROM esto permite a sitios web específicos enmarcar la página web en navegadores web compatibles).

5. **Referer expone ID de sesión:** Esto es un riego si la ID de sesión es sensible y el hipervínculo se refiere a un host externo o de un tercero. Para un contenido seguro, coloque la ID de sesión en la cookie de sesión segura.

6. **Error de formato de cadena:** tiene que reescribir el programa en segundo plano usando un borrador apropiado de las cadenas de caracteres erróneas. Esto requerirá el recompilado del ejecutable en segundo plano.

7. **Cookie sin atributo SameSite:** asegúrese de que el atributo SameSite este establecido en "lax" o idealmente estricto para todas las cookies.

8. **Cookie sin bandera asegurada:** Cuando una cookie contiene información sensible o es un token de sesión, debería ser siempre pasada usando un canal cifrado. Asegúrese que la bandera asegurada está establecida para cookies conteniendo información sensible.

9. **Divulgación de error de aplicación:** Revisar el código fuente de la página, implemente una página de error personalizada y considere implementar un mecanismo para proveer una única referencia de error para el cliente (navegador) mientras insertando los detalles en el sitio del navegador y no exponiéndolos al usuario.

10. **Incompleto o no Cache-control y sistema de encabezado HTTP Pragma:** Tienen que asegurarse que el encabezado HTTP cache-control este establecido con no-cache, no-store, must-revalidate y por último que el encabezado HTTP Pragma este establecido con no-cache.

11. **El servidor pierde información a través de los campos de encabezado de respuesta HTTP ''X-Powered-By'':** Asegúrese de que su servidor web, servidor de aplicaciones, equilibrador de carga, etc. Este configurado para suprimir los encabezados "X-Powered-By".

12. **Ausencia de tokens anti-CSRF:** para solucionar este tipo de ataque tiene que implementar cuatro (2) fase:
    - *Fase de Arquitectura y Diseño:* tiene que utilizar una biblioteca o un marco comprobado que no acepte que ocurra esta debilidad o que proporcione construcciones que permita que esta debilidad sea más sencilla de evitar. Ejemp. Utilice el paquete anti-CSRF.
      Origina un nonce único para cada uno de los formularios, coloque el nonce en el formulario y confirme la independencia al obtener el formulario, asegúrese de que el nonce no sea predecible (CWE-330). Tiene que tener en cuenta que esto puede pasar desapercibido utilizando XSS.
    - *Fase de Implementación:* tiene que asegurar que su aplicación esté libre de fallas de secuencias de comandos entre sitios, ya que la mayoría de las defensas de CSRF pueden detenerse por alto por medio del uso de secuencias de comandos manejados por el atacante.
      Revise que la solicitud se creó en la página esperada. Esto podría quebrar la funcionalidad autentica, ya que los usuarios o los representantes puede ser que hayan desactivado él envió de referer por motivos de privacidad.

Resumen

Se comprobó que la empresa AVANSI, SRL, aunque está certificada bajo la norma internacional ISO 27001, no está aplicando lo especificado en su Numeral 12.6 de Gestión de la vulnerabilidad técnica y el 12.6.1 control de las vulnerabilidades técnicas, se requiere una Reestructuración a nivel del servidor donde está almacenado la herramienta web de la Unidad de Registro (RA) en donde se gestionan los Certificados Digitales.

En cuanto a las vulnerabilidades encontradas durante esta auditoría se recomienda sean corregidas en un plazo de seis (6) meses. Luego del vencido dicho plazo, el INDOTEL verificará nuevamente las distintas vulnerabilidades con la intención de comprobar de que en efecto se haya corregido lo ante ya mencionado, en caso que se demuestre o se evidencie que dichas vulnerabilidades no fueron corregidas, se procederá a realizar una sanción según lo establece nuestra normativa vigente.

Luego de agotar todos los procesos existentes, con las excepciones encontradas durante el análisis de vulnerabilidades ejecutado con la herramienta OWASP-ZAP en el sitio web de la RA, **se evidenció que Avansi, SRL, ha cumplido de manera satisfactoria con los demás requerimientos que esta auditoría exige, incluyendo el resultado del primer control de vulnerabilidades ejecutado para el 2019, demostrando que la mayoría de sus procedimientos están siendo llevados de forma correcta y de acuerdo a lo establecido en la Ley No. 126-02 sobre Comercio Electrónico, Documentos y Firma Digital, su Reglamento de Aplicación y Normas Complementarias**.