INFORME TECNICO PREVIO DE EVALUACION DE SOFTWARE N°060-2019-GIN/SAT

1. NOMBRE DEL ÁREA:

Gerencia de Informática

2. RESPONSABLES DE LA EVALUACIÓN:

Juan Martin Camino Leon

3. CARGO / ROL:

Oficial de Seguridad de la Información

4. FECHA DE APROBACION

20 de junio del 2019

5. JUSTIFICACIÓN

Como soporte a las acciones estratégicas definidas en el Plan Estratégico Institucional (PEI) del Servicio de Administración Tributaria – SAT, se ha programado el desarrollo e implementación de aplicaciones y servicios web orientados a facilitar el acercamiento, comunicación e interacción del SAT con los ciudadanos y con otras entidades de la administración pública y privadas.

Es necesario tomar en cuenta que una vez publicada en Internet, toda aplicación web se encuentra potencialmente expuesta a una serie de amenazas, las cuales buscan explotar debilidades o vulnerabilidades en las aplicaciones para desarrollar actividades maliciosas que pueden generar riesgos para la seguridad de la información de las organizaciones. Por esta razón, toda aplicación web debe ser exhaustivamente analizada y testeada antes de su publicación y puesta en producción.

Como parte de los controles recomendados por la NTP ISO / IEC 27001:2014 Anexo A (A.12.6.1 Gestión de vulnerabilidades técnicas), en el SAT se desarrollan actividades de identificación, evaluación y corrección de las vulnerabilidades técnicas existentes sobre activos TI. Para ello se cuenta con herramientas que permiten automatizar este proceso con el fin de que resulte preventivo y se realice de forma permanente, evitando así que se materialicen riesgos que afecten la seguridad de la información en el SAT. La herramienta que se viene utilizando desde el año 2013 en el SAT es el scanner de vulnerabilidades NESSUS Professional y la plataforma de gestión de vulnerabilidades Tenable.IO Vulnerability Manager.

SAT Servicio de Administración Tributaria de Lima JUAN MARTIN CAMINO LEON Oficial de Seguridad de la Información

Con la finalidad de ampliar la cobertura de identificación de vulnerabilidades, se requiere implementar e integrar con las herramientas existentes, una herramienta que permita el análisis identificación y evaluación de riesgos de vulnerabilidades de las aplicaciones web durante la etapa de pruebas y desarrollo, para así corregirlas antes de su puesta en producción. Esto permitirá mitigar los riesgos asociados con ataques, explotación y uso indebido o no autorizado de estas aplicaciones

El presente informe se elabora en cumplimiento de la Ley N° 28612 Ley que norma el Uso, Adquisición y Adecuación del software en la Administración Publica, dejándose constancia que

la adquisición en cuestión responde a los principios de vigencia y neutralidad tecnológica, trasparencia y eficiencia, y a los criterios de austeridad y ahorro de los recursos públicos mencionados en dicha Ley.

6. ALTERNATIVAS

Considerando los requerimientos del SAT, se han tomado en cuenta las herramientas de software con mayor presencia en el mercado, que puedan cumplir con dichos requerimientos. Las alternativas que se sometieron a evaluación fueron las siguientes:

a. Acunetix Web Vulnerability Scanner
b. Qualys Guard Web App Security
c. Tenable.IO Web Application Scanning

Para el análisis de la información se han recurrido a las siguientes fuentes:

a. A través de la información disponible en la página web de los fabricantes:
b. Información disponible en Internet.

Cabe precisar que el requerimiento se genera sobre la necesidad de realizar el análisis de vulnerabilidades sobre aplicaciones web y que esta herramienta se complemente e integre con la herramienta de análisis de vulnerabilidades de activos TI con que actualmente cuenta el SAT.

7. ANALISIS COMPARATIVO TÉCNICO

El análisis técnico se ha realizado en conformidad con la metodología establecida en la "Guía Técnica de Evaluación de Software" aprobada por Resolución Ministerial Nº 139-2004-PCM:

a. **Propósito de la Evaluación:**

- Determinar los atributos o características mínimas más convenientes para asegurar que las alternativas evaluadas se ajustan a las necesidades y requerimientos del SAT.

b. **Identificar el tipo de producto**

- Software para análisis de vulnerabilidades de aplicaciones web

c. Especificaciones del modelo de calidad

Se aplicara el modelo de Calidad de Software Descrito en la parte I de la Guía de Evaluación de software aprobado por Resolución Ministerial Nº 139-2004-PCM.

d. Selección de Métricas

Las métricas fueron seleccionadas en base al análisis de los requerimientos del área de TI y a la información técnica de los productos de software señalados en el punto 6 Alternativas.

Del análisis realizado, se han determinado las siguientes características técnicas mínimas y sus respectivas métricas.

Item	Caracteristicas	Descripcion	Puntaje
Atributos Internos			
1	Adecuacion	Facilita la generacion de informes de vulnerabilidad estandar y de cumplimiento y provee una vista unificada	10
2	Integracion	Se integra y complementa con la plataforma de gestion de vulnerabilidades existente	10
Caracteristicas			
3	Seguridad	Testeo avanzado de Inyeccion SQL y Cross Site Scrpting	10
4	Conformidad de funcionalidad	Escanea y analiza sitios web en JAVA, .NET y PHP, incluyendo contenido HTML5, FLASH, SOAP Y AJAX	10
5	Automatizacion de tareas	Permite definir parámetros de frecuencia y horario para programar y automatizar el escaneo de aplicaciones web	10
6	Escaneo seguro	Exclusion de partes de las aplicaciones que se escanean a fin de prevenir interrupciones o latencias	10
Atributos externos			
7	Eficacia	Realiza escaneo inteligente , detecta el tipo de servidor y el lenguaje de la aplicación	10
8	Utilidad	Permite explorar un servidor web y ejecutar comprobaciones de seguridad contra los servicios de red que se ejecutan en el equipo	10
Atributos de uso			
9	Accesibilidad	Via Web , de acuerdo a roles	5
10	Compatibilidad	Compatibilidad con las ultimas versiones de los principales navegadores (Edge, Chrome, Mozilla)	5
11	Soporte	Del fabricante y del proveedor local	5
12	Capacitacion	Capacitacion en el uso y administacion del software proporcionada por el provedor local	5

SAT Servicio de Administración Tributaria de Lima
JUAN MARTIN CAMINO LEON
Oficial de Seguridad de la Información

Luego de determinar las características técnicas mínimas y las métricas aplicables, se procedió al análisis comparativo técnico, para lo cual se aplicó el modelo de calidad de software descrito en la Parte I Guía Evaluación de Software por Resolución Ministerial N° 139-2004 PCM.

Un aspecto importante que se ha tomado en cuenta al momento de la evaluación, es la integración con la plataforma de gestión de vulnerabilidades de activos TI que actualmente se encuentra en uso y con periodo de suscripción vigente (Tenable.IO Vulnerability Manager).

ITEM	CARACTERISTICAS	Acunetix WVS	Tenable IO WAS	Qualys WAS
1	Facilita la generacion de informes de vulnerabilidad estandar y de cumplimiento y provee una vista unificada	10	10	10
2	Se integra y complementa con la plataforma de gestion de vulnerabilidades existente	5	10	5
3	Testeo avanzado de Inyeccion SQL y Cross Site Scrpting	8	7	8
4	Escanea y analiza sitios web en JAVA, .NET y PHP, incluyendo contenido HTML5, FLASH, SOAP Y AJAX	8	9	8
5	Permite definir parámetros de frecuencia y horario para programar y automatizar el escaneo de aplicaciones web	10	10	10
6	Exclusion de partes de las aplicaciones que se escanean a fin de prevenir interrupciones o latencias	9	9	8
7	Realiza escaneo inteligente , detecta el tipo de servidor y el lenguaje de la aplicación	8	6	8
8	Permite explorar un servidor web y ejecutar comprobaciones de seguridad contra los servicios de red que se ejecutan en el equipo	8	8	8
9	Acceso via Web , de acuerdo a roles	5	5	5
10	Compatibilidad con las ultimas versiones de los principales navegadores (Edge, Chrome, Mozilla)	5	5	5
11	Soporte del fabricante y del proveedor local	5	5	5
12	Capacitacion en el uso y administacion del software proporcionada por el provedor local	5	5	5
PUNTAJES TOTALES		**86**	**89**	**85**

8. ANALISIS COSTO - BENEFICIO

Costos

Se requiere la suscripción de software para escaneo y análisis de vulnerabilidades web de 05 aplicaciones web por un periodo de doce (12) meses, además de capacitación y entrenamiento en el uso de la herramienta y aspectos de ciberseguridad que permitan obtener un mejor aprovechamiento de su uso.

No se ha realizado un análisis comparativo de costos, debido a que lo que se pretende es determinar la herramienta técnicamente más adecuada para atender los requerimientos de la institución. La evaluación formal de costos se realizara durante el proceso de adquisición correspondiente.

Las herramientas evaluadas son software cloud por lo que no requieren de hardware adicional para su explotación en el SAT.

Beneficio

La suscripción del software de análisis de aplicaciones web permitirá realizar una evaluación de riesgos de vulnerabilidades de las aplicaciones web durante la etapa de pruebas y desarrollo, permitiendo así corregirlas antes de su puesta en producción. De esta manera se amplía la cobertura de la gestión de vulnerabilidades técnicas que se lleva a cabo en el SAT lo cual permitirá mitigar los riesgos asociados con ataques, explotación y uso indebido o no autorizado de las aplicaciones web institucionales.

9. CONCLUSIONES

A partir de los resultados del análisis comparativo técnico desarrollado, se concluye que el software Tenable.IO Web Application Scanning (WAS), es el producto que mejor se ajusta a las necesidades de la entidad.

10. FIRMAS

Juan Martin Camino Leon
Oficial de Seguridad de la Información
SERVICIO DE ADMINISTRACION TRIBUTARIA DE LIMA