PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES

ADQUISICIÓN Y SOPORTE DE UNA SOLUCIÓN DE FIREWALL DE APLICACIONES WEB (WAF)

1.- OBJETO DEL CONTRATO.

Es objeto del presente expediente la contratación de una solución de Firewall de Aplicaciones Web (WAF por sus siglas en ingles) que ayude a proteger las aplicaciones web del Consorcio de Aguas Bilbao Bizkaia (CABB) contra ataques maliciosos y tráfico de Internet no deseado, como bots, inyección y denegación de servicio (denial of service, DoS) de capa de aplicación.

La contratación objeto del presente expediente constará, como mínimo, de los siguientes elementos:

- Licenciamiento y Software necesario para la implantación de la solución, cumpliendo los requerimientos del expediente.
- Servicios, que se dividirán en 3 fases:
    - Fase 1: Proyecto de puesta en marcha: Análisis, diseño, implantación, configuración, pruebas y puesta en producción de la solución, siguiendo las mejores prácticas indicadas por el fabricante. Protección inicial de 12 servicios web.
    - Fase 2: Servicios de soporte nivel 2 Correctivo/Reactivo y Preventivo/Evolutivo. Esta fase comenzará en la Fecha de Fin de Proyecto de la Fase 1.

2.- SITUACIÓN ACTUAL.

El CABB, desde su infraestructura on-premise, tiene publicados aplicaciones web en Internet de cara ofrecer diversos servicios tanto a clientes y proveedores, como a empleados del CABB para poder ejercer su labor diaria. Es necesario proteger dichas aplicaciones de posibles ataques que puedan desde impedir su uso hasta acceder y manipular la información de las mismas.

3.- ORGANIZACIÓN

La empresa adjudicataria deberá disponer de la organización y medios técnicos, humanos y materiales necesaria para poder acometer con éxito los servicios solicitados, para lo que deberá componer un grupo de trabajo que cuente con un responsable coordinador del servicio, especialista en Seguridad, Comunicaciones e Internet.

4.- PLANTEAMIENTO DEL SERVICIO

Fase 1: Proyecto de puesta en marcha

Puesta en marcha: Se consideran incluidas en esta fase todas las tareas necesarias para la óptima puesta en producción de la solución ofertada, incluidas la adquisición de licencias, instalación y configuración de las maquinas virtuales necesarias y definición de políticas y su puesta en marcha para 12 servicios Web.

Traspaso de Conocimiento/Formación: Se efectuará durante un mínimo de 10 horas, en un mínimo de 2 jornadas, el traspaso de información destinado al personal técnico del CABB, que permita adquirir los conocimientos relativos a arquitectura, funcionalidades, configuración, explotación, administración y mantenimiento de la plataforma implementada.

Fecha de fin de puesta en marcha: Es la fecha en la que se dará por finalizada la Fase 1, que coincidirá con la fecha del acta de reunión de fin de proyecto.

Fase 2: Servicios de soporte nivel 2 Correctivo/Reactivo y Preventivo/Evolutivo

Servicio Correctivo/Reactivo.

Se entiende por incidencia cualquier petición o consulta debido a un problema en el sistema, incluida en el ámbito del expediente, realizada por el CABB al contratista, incluida la detección de vulnerabilidades que impliquen una rápida actualización del sistema o cambios en la configuración para mitigarlas.

De cara al planteamiento del servicio, se clasifican las incidencias de la siguiente manera:

Prioridad	Impacto	Ejemplo
Crítica	Impacto grave en las operaciones, caída del servicio. El cliente o un grupo de trabajo no pueden realizar sus tareas habituales. Los servicios de producción u otros sistemas críticos se encuentran parados, y no se ha encontrado una solución de forma inmediata.	Servicio no disponible.
Urgente	Pérdida de una funcionalidad importante, servicio en riesgo. Alguna de las funcionalidades principales se encuentra dañada, lo que provoca una degradación del rendimiento del sistema en general o de un grupo de trabajo.	El problema crea retrasos inasumibles en la disponibilidad del servicio.
Leve	Impacto bajo en la productividad, bajo rendimiento. La solución es conocida pero el problema debe ser resuelto. Implica una pérdida parcial y no critica de funcionalidad.	La incidencia no produce ningún tipo de problemas o produce una perdida asumible en la disponibilidad de los servicios.

Servicio Preventivo/Evolutivo

Se realizará una revisión **mensual** de la plataforma en la que se realizará un análisis de su estado de salud, así como recogida de métricas e inventario de la configuración de cara a la elaboración de un informe mensual en el que vengan reportadas.
Dicho informe también incluirá una relación de las incidencias reportadas en el último periodo, así como su resolución o estado en dicho momento.
El informe también incluirá recomendaciones a nivel evolutivo o de mejora.
Durante la revisión mensual, se podrán realizar modificación de configuraciones bajo aprobación del CABB, que no supongan cambios en la arquitectura o infraestructura.
Se realizará también una revisión de versiones del sistema y actualización de las mismas (bajo aprobación del CABB) en caso de que se vea necesario.

Se podrán realizar también pruebas periódicas de contingencia y/o continuidad del servicio.

Documentación. La documentación a generar por el contratista durante la duración del contrato constará como mínimo de:

Fase 1: Proyecto de puesta en marcha

- Actas de reuniones de inicio y seguimiento de proyecto.
- Documento de diseño y requerimientos, que incluya esquema de componentes y conexiones entre ellos, funcionalidades a implementar y configuración a aplicar para cada uno de los componentes, plan de proyecto que incluya fases, hitos, plazos de ejecución y planificación.
- Finalización. El CABB dará el visto bueno y por finalizada la fase 1 del proyecto tras realizar la entrega por parte del contratista al CABB de la documentación final que constará, como mínimo, de:
    - Documento final de proyecto, con esquema y detalle de la arquitectura final y componentes instalados, interconexiones entre ellos, configuración, políticas definidas, resultado de las pruebas realizadas y situación final de las soluciones implementada.
    - Acta de reunión de fin de proyecto.
    - Certificados de titularidad de los elementos incluidos en la oferta.
    - Planificación de chequeos de salud, entrega de informes y reuniones y puntos de control, para toda la duración del contrato.

Fase 2: Servicios de soporte nivel 2 Correctivo/Reactivo y Preventivo/Evolutivo.

- Acta de reunión de inicio del servicio.
- Documento de procedimiento de apertura y cierre de solicitudes por parte del CABB al contratista.
- Actas de reuniones de seguimiento del servicio.
- Informes periódicos de mantenimiento Preventivo/Evolutivo del servicio que incluirán:
    - Inventario de equipamiento. Estado de los elementos de la plataforma (rendimiento, versionado, etc.). Se recopilarán y mantendrá actualizado el inventario del equipamiento en el alcance del servicio y se reflejará cualquier cambio que se dé sobre el mismo en lo que respecte tanto a la parte de licenciamiento y soporte como versiones y número de elementos que la componen.
    - Incidencias reportadas. Se referenciarán todos los incidentes solucionados en el periodo en estudio indicando, además, para aquellos clasificados como críticos, las causas, fechas y acciones realizadas para su resolución.
    - Incidencias destacadas y su solución técnica a lo largo del periodo en estudio.
    - Recomendaciones. Se incluirán las conclusiones de las revisiones periódicas correspondientes a los procesos de inspección periódica planteados dentro del contrato, con el detalle de las actuaciones realizadas y las recomendaciones de mejora sugeridas en cada caso.

5.- ACUERDOS DE NIVEL DE SERVICIO

Fase 1: Proyecto de puesta en marcha

Plazo de puesta en marcha: El plazo de puesta en marcha será como máximo de 3 meses desde la firma del contrato.
Fecha de Finalización. Será la fecha del acta de fin de proyecto en la que se dará por finalizada la Fase 1.

Fase 2: Servicios de soporte nivel 2 Correctivo/Reactivo

SERVICIOS DE SOPORTE NIVEL 2 CORRECTIVO/REACTIVO

Prestación del Servicio. El servicio se prestará en las siguientes modalidades, según la prioridad de las incidencias, para todos los elementos de la solución ofertada:

- 8 x 5: de 8h a 14:00h y de 15:00 a 17:00h, de lunes a jueves y viernes de 8h a 15h.
- NBD: Next Business Day.

Tiempo de Atención. Se entiende por Tiempo de Atención el tiempo transcurrido entre el conocimiento de la incidencia o solicitud por parte del contratista, o en todo caso por su notificación por parte del CABB, y la atención de un técnico especializado en la plataforma.

Tiempo de Resolución Se entiende por Tiempo de Resolución el periodo de tiempo que media entre el conocimiento de la incidencia o solicitud por parte del contratista, o en todo caso por su notificación por parte del CABB, y la finalización de la realización de lo solicitado o resolución total de la incidencia.

- Incidencias

Prioridad Incidencias	Modalidad de Servicio	Tiempo de Atención (horas)	Tiempo de Resolución (horas)*
Crítica	8x5	1	2
Urgente	8x5	2	4
Leve	NBD	2	8

* El contratista deberá adscribir personas con roles y dedicación necesarios para que la resolución de la incidencia se corresponda con los tiempos indicados, incluyendo el seguimiento de la incidencia en el caso de que sea necesaria la intervención del fabricante para su resolución.

6.- REQUERIMIENTOS TÉCNICOS

La solución ofertada deberá de cumplir, en el momento de presentación de la oferta, con los siguientes requerimientos.

CARACTERÍSTICAS DE SUSCRIPCIÓN Y RENDIMIENTO

- Sistema operativo de propósito específico (no de propósito general), desarrollado por el fabricante específicamente para funciones de balanceo de carga de servicios, aplicaciones IP (TCP/UDP) y servicios web.
- Se desplegará mediante maquinas virtuales (OVA) en la infraestructura VMWare del CABB, aunque debe tener la posibilidad de desplegarse mediante appliance físico.
- Características mínimas de rendimiento:
  - Throughput nominal: 200Mb para balanceo en condiciones de carga máxima
  - Soporte de claves SSL de 1024, 2048 y 4096 bits

  - Soporte de AES, AES-GCM, SHA1/MD5 y algoritmos de llave pública: RSA, Diffie-Hellman, Digital Signature Algorithm (DSA) y Elliptic curve cryptography (ECC)
  - Firmado criptográfico de cookies para verificar su integridad
- Soporte de alta disponibilidad. Aunque no se contempla su necesidad inicial en el proyecto, debe poder soportar su instalación en cluster con las siguientes características:
  - Clúster activo-pasivo con un grupo de fail-over de hasta 8 dispositivos físicos o virtuales
  - Clúster activo-activo entre dos o más plataformas permitiendo cualquier combinación entre equipos hardware de diferentes modelos, máquinas virtuales o instancias virtuales dentro de dispositivos físicos
  - Sincronización de configuración tanto automática como manual entre equipos hardware de diferentes modelos, máquinas virtuales e instancias virtuales dentro de dispositivos físicos de hasta 32 elementos
  - Decisión de fail-over entre plataformas heterogéneas basada en recursos y tráfico actual

INTEGRACIÓN EN RED

- Estándares de red soportados: VLAN 802.1q, 802.3ad, NAT, sNAT, IPV6 (incluyendo función de gateway entre redes IPv6-IPv4), rate shapping, dominios de enrutamiento independientes con capacidad de solapamiento de direccionamiento IP
- Creación de túneles IPSEC LAN-to-LAN y certificación por ICSA Labs como dispositivo IPSEC 1.3

ADMINISTRACIÓN DEL SISTEMA

- Sistema de administración totalmente independiente del sistema de procesamiento de tráfico
- Administración del equipo vía CLI (Interfaz de Línea de Comandos) por SSH
- Administración del equipo vía interfaz de administración gráfica basada HTTPs
- Integración con Directorio Activo Windows 2003 o superior, LDAP, RADIUS
- Comunicación cifrada con el dispositivo y autenticación de los usuarios administradores/supervisores con certificados digitales
- Soporte de envío de alertas y eventos a un sistema centralizado mediante:
  - Protocolo SysLog y High Speed Logging
  - Notificación vía SMTP
  - SNMP versión.2.0 o superior
- Interfaz gráfica con dashboard personalizable que permita monitorizar el estado del equipo en tiempo real
- Módulo de reportes que permita visualizar gráficamente el comportamiento de las aplicaciones web: latencias y throughput hacia los servidores, latencias en los URLs, direcciones IP origen, URLs más visitados y otras estadísticas de los servicios balanceados y los servidores
- Plantillas para la implementación rápida de aplicaciones de mercado conocidas (al menos Microsoft, WordPress, Apache, Tomcat) y posibilidad de creación de plantillas personalizadas que puedan ser actualizadas/exportadas entre equipos
- Gestión y monitorización mediante API REST permitiendo integración tanto imperativa como declarativa (configuración de un servicio completo mediante una única llamada REST)
- Automatización mediante módulos Ansible soportados por el fabricante
- Posibilidad de sincronización de configuración incremental

WEB APPLICATION FIREWALL (WAF)

- Protección de las aplicaciones y servicios web ante ataques a nivel de aplicación y ataques de denegación de servicio de nivel 7 de manera proactiva (Web Application Firewall) en el mismo dispositivo de balanceo:

- Certificación ICSA como firewall de aplicación (WAF)
- Política de seguridad:
  - Funcionamiento en esquema de proxy TCP reverso y/o transparente
  - Funcionamiento en modo de bloqueo o transparente
  - Soporte de modelos de seguridad positiva y negativa
  - Aplicación de políticas por servicio virtual
  - Firmas nativas para tecnologías de servidor de mercado (al menos Nginx, PHP, Apache, Wordpress, Handlebars)
  - Creación de firmas personalizadas
  - Soporte para creación automática de políticas, incluyendo políticas basadas en wildcards con múltiples URLS
  - Políticas en base al aprendizaje del comportamiento de la aplicación automáticamente sin intervención humana
  - Política de seguridad para API mediante una configuración guiada e importación de un archivo swagger y OpenAPI
  - Creación y despliegue de políticas de seguridad, protección antiBots y protección frente a denegación de servicio mediante wizards
  - Administración de las políticas de seguridad mediante una API declarativa
  - Soporte para comparar dos políticas y mostrar las diferencias entre ambas
  - Personalización de las páginas de bloqueo con capacidad de responder a webservices mediante un código HTTP 500
  - Posibilidad de restringir cada uno de los siguientes parámetros:
    - Protocolo y versión utilizada
    - Longitud del método de request
    - Longitud del URI solicitado
    - Número de cabeceras (headers)
    - Longitud del nombre de las cabeceras
    - Longitud del valor de las cabeceras
    - Longitud del cuerpo (body) de la solicitud
    - Longitud del nombre y el valor de las cookies
    - Número de cookies
    - Longitud del nombre y valor de los parámetros
    - Número de parámetros
  - Soporte de multi-byte language encoding
  - Validación de URL-encoded characters
- Programabilidad:
  - Soporte de scripts de programación basados en lenguaje estructurado TCL para configuraciones fuera de las funcionalidades/opciones por defecto
  - Soporte de extensiones de Node.js para extender las funcionalidades del plano de datos y del plano de control del equipo
- Mecanismos de identificación y protección básicos:
  - Top 10 de OWASP
  - Ataques de Fuerza Bruta
  - Cross-site scripting (XSS)
  - Cross Site Request Forgery
  - SQL injection
  - Parameter and HPP tampering
  - Sensitive information leakage
  - Session highjacking

  - Buffer overflows
  - Cookie manipulation
  - Various encoding attacks
  - Broken access control
  - Forceful browsing
  - Hidden fields manipulation
  - Request smuggling
  - XML bombs/DoS
  - Open Redirect
  - Protección específica contra ataques HTTP Desync
- Mecanismos de identificación y protección avanzados:
  - Generación de firmas dinámicas de capa 7 en tiempo real para la mitigación de ataques de DDoS incluyendo detección dinámica de latencias del servidor
  - Soporte de análisis de comportamiento para la mitigación de DDoS de nivel 7 en un número ilimitado de servicios
  - Protección frente ataques de DDoS en la negociación de TLS mediante fingerprinting del stack TLS presentado por el cliente
  - Protección mediante cifrado de los campos sensibles de las aplicaciones web en el navegador cliente
  - Garantía de integridad de datos, detectando al menos la manipulación de parámetros en URLs y peticiones AJAX
  - Protección anti-bot con mecanismos de captcha y challenge de javascript para detección e identificación de navegadores y comportamiento de usuario
  - Protección frente a Web Scraping
  - Identificación de URLs con gran consumo en los servidores como vector de ataque de DDoS
  - Verificación de las firmas de ataque en las respuestas del servidor al usuario
  - Enmascaramiento de información sensible enviada por el servidor
  - Bloqueo basado en la ubicación geográfica (base de datos de geolocalización incluida)
  - Descarte de paquetes de una IP sospechosa una vez detectado un ataque
  - Verificaciones de seguridad y validación en protocolos FTP y SMTP
  - Protección a Web Services XML y restricción al acceso mediante métodos definidos vía Web Services Description Language (WSDL)
  - Soporte para prevenir exponer el “OS fingerprinting”
  - Soporte de tecnologías AJAX y JSON
  - Opción de alimentarse de una base de datos de reputación de IPs (aunque sea susceptible de activarse a futuro) que permita bloquear tráfico desde y hacia direcciones IP en categorías como: scanners, Windows exploits, denial of services, proxies de phishing, botnets, proxies anónimos
- Monitorización, informes y diagnóstico:
  - Panel de control de cumplimiento del Top 10 OWASP
  - Reportes de cumplimiento de la normativa PCI DSS 3.2
  - Posibilidad de captura de tráfico con tcpdump en caso de ataque
  - Mecanismos de auditoría de cambios
- Integraciones requeridas:
  - Integración con herramientas de verificación de vulnerabilidades (al menos WhiteHat, Qualys, IBM AppScan, HP WebInspect.s)
  - Integración con servidores Antivirus por medio del protocolo ICAP
  - Integración con firewalls de bases de datos. Al menos IBM InfoSphere Guardium y Oracle Database Firewall

- Opciones susceptibles de activarse a futuro:
  - Suscripción a un feed para protección de campañas de ataque activas en Internet
  - Detección y mitigación de tráfico de bots basada en Inteligencia Artificial y Machine Learning mediante un javascript ofuscado

7.- PROPUESTA TÉCNICA

Se deberá presentar, y se valorará, la propuesta técnica para la solución, en la que se presentarán los siguientes aspectos:

- Solución ofertada.
- Fase 1: Proyecto de puesta en marcha.
- Fase 2: Servicios de soporte nivel 2 Correctivo/Reactivo y Preventivo/Evolutivo.

Solución ofertada

Se detallarán los siguientes aspectos de la solución ofertada:

- Arquitectura.
- Componentes.
- Funcionalidades.
- Seguridad.
- Usabilidad.
- Herramientas de gestión.
- Estadísticas e informes.

Se detallará también el modo de licenciamiento de la solución ofertada.

Fase 1: Proyecto de puesta en marcha

Se detallará el planteamiento realizado para la puesta en marcha de la solución, teniendo en cuenta, como mínimo, los siguientes aspectos:

- Plan de proyecto.
- Planificación por fases.
- Hitos a cumplir.
- Pruebas a realizar.
- Documentación a generar.
- Formación a los técnicos del CABB.
- Equipo técnico asignado al proyecto.

Fase 2: Servicios de soporte nivel 2 Correctivo/Reactivo y Preventivo/Evolutivo.

Se detallará el planteamiento realizado para realizar el soporte Correctivo/Reactivo y Preventivo/Evolutivo de la solución, teniendo en cuenta, como mínimo, los siguientes aspectos:

- Servicios de soporte nivel2 Correctivo/Reactivo. Se debe indicar el alcance del servicio de mantenimiento y soporte donde se describa claramente:
  - Modelo del servicio, indicando el equipo técnico asignado a la ejecución del servicio de mantenimiento Correctivo/Reactivo durante toda la duración del contrato.
  - Metodología y procedimientos para la prestación de los servicios de soporte:
    - Procedimientos operativos en la prestación de los servicios solicitados.
    - Flujo y canales de comunicación.

        - Métricas y SLAs.
        - Gestión, control y aseguramiento de la calidad del servicio prestado.
        - Gestión y seguimiento del contrato.
- Servicios de soporte Preventivo/Evolutivo. Se debe indicar el detalle de las tareas, tanto proactivas como evolutivas incluidas en la oferta, que serán como mínimo las siguientes:
    - Inventario de equipamiento y políticas.
    - Informe de incidencia reportadas.
    - Recomendaciones evolutivas sobre la plataforma.
    - Métricas a recoger y documentación a generar.
    - Equipo técnico asignado al servicio.

Bilbao, 30 de octubre de 2024

El Gestor del Contrato
David Alonso Villafáfila

Subdirector de Informática
Jose Luis Unzueta