Expediente nº: 2022019

Objeto de la contratación: Servicio de "*Pentesting*" para el Basque CyberSecurity Centre

Documento: Pliego de prescripciones técnicas particulares

Contenido

1. CONTEXTO 3
2. OBJETO DE LA CONTRATACIÓN 3
3. DESCRIPCIÓN DEL SERVICIO 3
4. ALCANCE 4
5. CARACTERÍSTICAS DEL SERVICIO 4
5.1. Metodología 4
5.2. Planificación 5
5.3. Entregables 5
5.4. Equipo de trabajo 6
6. CONDICIONES PARA LA PRESTACIÓN DEL SERVICIO 6

1. CONTEXTO

El BASQUE CYBERSECURITY CENTRE (en adelante, **BCSC**), es una iniciativa que se enmarca dentro de la Agencia Vasca De Desarrollo Empresarial - Enpresen Garapenerako Euskal Agentzia (en adelante SPRI), ente público de derecho privado dependiente del Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente del Gobierno Vasco.

El BCSC, como unidad de SPRI, es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

El BCSC es un instrumento del Gobierno Vasco para elevar la cultura de la ciberseguridad en la sociedad vasca y aspira a erigirse como punto de encuentro entre oferentes y demandantes de servicios especializados, generando con ello una oportunidad para la innovación, potenciando la competitividad de las empresas y facilitando que la ciudadanía desarrolle hábitos para una actividad digital más segura.

Para alcanzar sus objetivos, el BCSC se define como una iniciativa transversal que desde su inicio involucra a cuatro Departamentos del Gobierno Vasco, el ya antes citado de Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente, el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación. La actividad abarca proyectos de investigación, iniciativas de emprendimiento y colaboración coordinada con otros agentes competentes a nivel estatal e internacional. No en vano se trabaja en estrecha colaboración con agentes de la Red Vasca de Ciencia Tecnología e Innovación que forman parte de Comité Permanente del BCSC.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución proyectos de colaboración entre actores complementarios en los ámbitos de la innovación tecnológica, de la investigación y de la transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

El BCSC ofrece diferentes servicios en su rol como Equipo de Repuesta a Incidentes (en adelante CSIRT, por sus siglas en inglés “Computer Security Incident Response Team”) y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar su capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca.

2. OBJETO DE LA CONTRATACIÓN

El objeto del expediente es la contratación de un servicio de Pentesting que permita identificar las debilidades y los fallos presentes en la infraestructura TIC del BCSC. Del mismo modo, se deberán proponer las medidas adecuadas para eliminar o mitigar los riesgos de estas.

3. DESCRIPCIÓN DEL SERVICIO

En este apartado se describen las características técnicas que conforman el objeto del contrato y que el adjudicatario deberá prestar, no siendo el listado que aparece a continuación una relación exhaustiva de las características del servicio contratado, sino las actividades generales demandadas por el BCSC, cubriendo los aspectos mínimos de tareas a realizar y resultados esperados.

Los referidos requisitos deben entenderse como mínimos (a excepción de que se indique lo contrario) pudiendo los licitadores ampliarlos en sus ofertas.

El licitador deberá aportar y describir los conocimientos, metodologías, herramientas y equipo humano en el que se apoyará para asegurar el resultado óptimo del proyecto.

El adjudicatario se obligará a guardar secreto y a hacerlo guardar al personal que emplee para la prestación del servicio, respecto a toda la información que con motivo del desarrollo de los trabajos llegue a su conocimiento, no pudiendo utilizarla para sí o para otra persona o entidad.

4. ALCANCE

La empresa licitadora deberá detallar el número máximo de activos que podrán ser objeto de las pruebas de intrusión, este **alcance** no podrá ser inferior a:

- 60 servidores
- 15 IPs externas
- 2 SSID

5. CARACTERÍSTICAS DEL SERVICIO

5.1. Metodología

La empresa licitadora deberá plantear las **metodologías** más apropiadas para la realización del test de penetración, deberá incluir en qué buenas prácticas de la industria se basa y recogerá aspectos como alcance de cada área de la auditoría, los aspectos a auditar, cómo hacerlo, los resultados que se espera generar y las capacidades profesionales de los realizadores para cada ámbito.

La propuesta deberá contemplar, al menos, la realización de los siguientes tipos de evaluaciones:

- Análisis completo de la superficie de ataque a partir de las IPs externas indicadas.
- Test de intrusión en la red desde Internet.
- Auditoría técnica de seguridad tipo caja gris en la red interna que contemple, al menos, los siguientes niveles:
    - Red:
        - Obtención de información de los sistemas mediante el escaneo de redes. Identificar servicios (por lo puertos TCP o UDP abiertos) y sistemas (por el contenido de paquetes).
        - Análisis en profundidad los dispositivos de protección perimetral (routers, cortafuegos, etc.…).
    - Sistema operativo (SO) y plataforma:
        - Análisis de la capacidad de resistencia de los sistemas identificados ante intentos de intrusión, explotación de vulnerabilidades o realización de movimientos laterales entre maquinas.
    - Grupos, roles y políticas:
        - Verificación de la configuración de los grupos, roles y políticas para los diferentes perfiles de usuario.
- Auditoría de seguridad de redes WiFi que contemple, al menos, los siguientes aspectos:
    - Descubrimiento los SSIDs en uso dentro de la red.
    - Identificación de los puntos de acceso utilizados para el acceso a la red inalámbrica.

- Realización de un análisis WLAN en busca de redes inalámbricas no autorizadas.
- Análisis la capacidad de romper la red inalámbrica corporativa desde la red inalámbrica de invitados.
- Análisis de la configuración de infraestructura wifi accesible como usuario.
- Análisis del portal web de onboarding.
- Evaluación de la dispersión de la señal más allá de la oficina.

No se admitirán únicamente ataques con herramientas automáticas, si bien si será posible utilizarlas como herramientas de apoyo siempre y cuando quede reflejado en el informe técnico indicado en el apartado 5.3 siguiente y se entreguen los resultados como anexo al citado informe técnico.

5.2. Planificación

La empresa licitadora deberá realizar una propuesta de **plan de trabajo**, reflejando los hitos más relevantes del servicio con sus respectivas fechas, así como el flujo de ejecución/operación que se aplicaría en el momento de ejecutar las actividades.

5.3. Entregables

La empresa licitadora deberá especificar los **entregables** con una descripción y estructura aproximada de lo que incluirá cada uno de ellos.

Se solicitan, al menos, los siguientes entregables:

- Plan de auditoría, donde se detalle al menos, las pruebas a realizar, la organización temporal e impactos posibles.
- Informe ejecutivo, donde se resuma la información más relevante del informe técnico para su escalado a mandos superiores.
- Informe técnico, especificando para cada área, sistema o grupo de sistemas análogos:
  - Objetivo de la auditoría con la identificación de lo auditado.
  - Proceso metodológico y herramientas aplicadas.
  - Tipología y estructura de las pruebas realizadas.
  - Histórico de las pruebas realizadas referenciando los TTPs utilizados.
  - Identificación univoca de deficiencias / vulnerabilidades identificadas
  - Clasificación de riesgo de los hallazgos según marco de referencia y propuesta de priorización apoyada en el contexto obtenido durante la actividad a la hora de abordar su resolución.
  - Datos, hechos y observaciones en que se basen los dictámenes alcanzados.
  - Plan de acción detallando las medidas correctoras o complementarias necesarias para eliminar o mitigar los riesgos identificados.
  - Evidencias y ejemplos para aquellas pruebas que deriven en un riesgo de seguridad clasificado como alto o crítico de forma que sea posible reproducirlas de manera autónoma por el personal del BCSC.

El formato del informe debe ser particularizado y contextualizado al entorno del BCSC, a los hallazgos obtenidos, metodologías utilizadas y actividades realizadas, no admitiéndose el uso de informes automáticos generados por herramientas. En caso de haber utilizado herramientas automáticas como apoyo, los informes "en bruto" deben ser entregados como anexos al informe técnico.

A modo de muestra, **el licitador deberá presentar un ejemplo de los tres entregables solicitados**, así como de cualquier otro que se quiera añadir, **como anexo_2 a la oferta técnica**.

Los ejemplos referidos en el apartado anterior podrán consistir bien en entregables de idénticas o similares características que los licitadores hayan desarrollado para actuaciones precedentes y para clientes / usuarios distintos de BCSC, o bien en informes sistémicos que actuarán a modo de boceto de los entregables indicados en el presente apartado.

5.4. Equipo de trabajo

La empresa licitadora deberá detallar el **equipo de trabajo** disponible para la ejecución del contrato, indicando para cada recurso el perfil y rol al que se asocia, así como su experiencia en actividades similares para asegurar la correcta prestación del servicio.

Los componentes del equipo de trabajo deberá acreditar un **mínimo de 5 años de experiencia** y se valorará que cuenten con certificaciones que acrediten los conocimientos necesarios para la ejecución de los trabajos (GXPN, GWAPT, GPEN, GAWN, LPT, OSCP, OSWE, PenTest + o similares).

El equipo de trabajo a incorporar tras la formalización del contrato para la ejecución de los trabajos deberá ser el detallado en la oferta adjudicataria y consecuentemente valorado, debiendo acreditarse, en caso de adjudicación, las certificaciones expuestas como argumento para la valoración.

Las características del equipo de trabajo se justificarán mediante la utilización de la tabla *Anexo1_EquipoTrabajo*, tal como se indica en el pliego de cláusulas administrativas.

6. CONDICIONES PARA LA PRESTACIÓN DEL SERVICIO

A continuación, se enumeran las condiciones en las que el licitador deberá prestar los servicios solicitados

- El horario para la realización de las pruebas de intrusión será acordado con el BCSC, como referencia de 8.30am a 17.30pm, si bien para aquellas pruebas que puedan impactar en sistemas críticos el BCSC, BCSC podrá, a su criterio exclusivo, solicitar la realización de las pruebas fuera del horario laboral.
- Para acceder a los sistemas en las ubicaciones del BCSC, desde el BCSC se proporcionarán los medios para posibilitar el acceso y las comunicaciones entre la infraestructura y sistemas del BCSC y los del adjudicatario mediante el uso de VPN.
- Las pruebas de caja gris de la red interna podrán realizarse tanto desde las instalaciones de la empresa licitadora, como desde las propias instalaciones del BCSC, en el caso de optar por la segunda opción desde el BCSC se facilitará el acceso a las instalaciones y un entorno adecuado para desplegar los equipos necesarios.
- Para la verificación de la configuración de los grupos, roles y políticas para los diferentes perfiles de usuario, desde el BCSC se facilitarán las credenciales correspondientes.
- Para las pruebas del entorno Wifi será necesario la presencia *In-situ* en las instalaciones del BCSC. A tales efectos, desde el BCSC se facilitará el acceso a las instalaciones y un entorno adecuado para desplegar los equipos necesarios.

- El licitador asumirá dentro de los costes del proyecto cualquier gasto derivado de desplazamiento del equipo a las instalaciones del BCSC, no pudiendo solicitar compensación alguna por ello.
- El licitador deberá estar en posesión de aquellas certificaciones, autorizaciones y permisos que sean exigibles por la legislación vigente para la prestación de los servicios solicitados.