



Eusko Jaurlaritzaren
Informatika Elkarte

Sociedad Informática
del Gobierno Vasco

Expediente nº EJIE-002-2024

Provisión de un servicio operativo de cibervigilancia para las elecciones autonómicas de Euskadi 2024

Pliego de Condiciones Técnicas

Diciembre de 2023

Este documento es propiedad de Eusko Jaurlaritzaren Informatika Elkarte – Sociedad Informática del Gobierno Vasco, S.A. (EJIE) y su contenido es CONFIDENCIAL. Este documento no puede ser reproducido, en su totalidad o parcialmente, ni mostrado a otras partes, ni utilizado para otros propósitos que los que han originado su entrega, sin el previo permiso escrito de EJIE. En el caso de ser entregado en virtud de un contrato, su utilización estará limitada a lo expresamente autorizado en dicho contrato. EJIE no podrá ser considerada responsable de eventuales errores u omisiones en la edición del documento.

Versión	Fecha	Resumen de cambios	Elaborado por	Aprobado por
1.0	22/12/2023	Versión inicial	Seguridad Corporativa	Agustín Moyano

Índice

1 **Introducción** 4

 1.1 Perfil de la compañía 4

2 **Situación actual** 5

3 **Objeto del contrato**.....6

 3.1 Objeto y alcance del servicio 6

4 **Fases a cubrir** 7

 4.1 Etapa de preparación 7

 4.2 Etapa de activación 8

 4.3 Etapa posterior a la jornada electoral 8

5 **Requisitos tecnológicos** 9

 5.1 Capacidades de la plataforma de deception 9

6 **Entregables** 11

1 Introducción

1.1 Perfil de la compañía

EJIE, Eusko Jaurlaritzaren Informatika Elkartea – Sociedad Informática del Gobierno Vasco, es la Empresa pública de servicios de las tecnologías de la información y las comunicaciones (TIC), cuya razón de existir es contribuir a la consecución de un Sector Público Vasco, moderno y eficiente, en el Marco Legal establecido por el Gobierno, con la seguridad y calidad necesarias y con el debido respeto al medio ambiente.

EJIE tiene como meta final la consecución de la satisfacción de sus clientes, siendo el instrumento común de prestación de servicios TIC en el Sector Público Vasco, y comprometiéndose en:

- Construir y mantener con eficiencia y calidad la infraestructura de los Sistemas de Información, posibilitando su continuidad y seguridad.
- Garantizar la interoperabilidad entre las distintas administraciones.
- Servir de apoyo a las necesidades de planificación y realización de la función informática de los Departamentos y Organismos Autónomos del Gobierno, asegurando la cobertura de sus demandas con el compromiso y profesionalidad adecuados a las relaciones contractuales que se establezcan.

Por tanto, EJIE debe ser, un instrumento común de referencia para la prestación de servicios TIC en el Sector Público Vasco:

- Aportando valor añadido.
- Proporcionando soluciones competitivas.
- Transmitiendo confianza a sus clientes.
- Contando con personas cualificadas y comprometidas.

Se puede obtener información más detallada y extensa en nuestra dirección de Internet <https://www.ejie.eus>.

2 Situación actual

A lo largo del año 2024 se van a celebrar elecciones autonómicas en Euskadi y existe una situación geopolítica que incita a pensar que es un evento que debe ser tratado de manera especial en materia de ciberseguridad, dado que la probabilidad de intentos de intrusión, interacción o alteración de dicho proceso no es menor.

Este hecho, así como el carácter extraordinario de las elecciones, supone un aumento de la posibilidad de recibir ciberataques sobre los sistemas de información corporativos y sobre los sistemas específicos puestos en marcha para el proceso electoral, y el consecuente aumento del riesgo de seguridad asociado.

La cibervigilancia tiene como objeto prevenir actividad maliciosa con ocasión de las elecciones. A tal efecto se requiere monitorizar:

- Las identidades digitales conocidas del universo de actores de ciberdelincuencia que operan en cualquier país y en los idiomas de interés.
- Contenidos relevantes a las elecciones, circulando por canales digitales conectados a Internet en una esfera pública o en espacios donde puede realizarse una autenticación sin métodos invasivos ni ilegales
- Estos canales incluyen tanto sitios web, como la diversidad disponible de redes sociales en los idiomas de interés, mercados de compraventa de activos digitales, conversaciones establecidas con identidades de interés o utilización de herramientas públicas para conocer el estado de situación en varios ámbitos (por ejemplo, el registro de nuevos dominios web, la divulgación de vulnerabilidades o de exploits).

A tal efecto, Ejie ha diseñado un operativo especial de ciberseguridad para gestionar las posibles situaciones.

3 Objeto del contrato

3.1 Objeto y alcance del servicio

Para hacer frente a posibles ciberataques, focalizar los esfuerzos de los equipos operativos de forma efectiva y poder reportar con un lenguaje común y sencillo se han identificado las siguientes amenazas:

- Hacktivismo
- Ataques DDoS
- Defacement
- Robo de datos y filtraciones
- Desinformación
 - Fake news
 - Amplificación de la información
 - Postverdad (mentira emotiva)
- Cualquier otro tipo de ciberataque

Para garantizar la protección, prevención y respuesta tanto en los activos del Ejie/Gobierno Vasco como en el ámbito del proceso electoral se han tenido en cuenta los siguientes objetivos:

- Monitorización de los sistemas de información vinculados al proceso electoral
- Monitorización específica y gestión de vulnerabilidades
- Aplicación de contramedidas e investigación de incidentes de seguridad
- Detección e identificación de las ciberamenazas
- Establecimiento del modelo de coordinación y comunicación

Se han identificado una serie de acciones en los siguientes ámbitos:

- Proceso electoral: activos que sustentan los procesos fundamentales del proceso electoral y que se convierten en esenciales. Algunos de estos procesos son la captura de datos o el recuento de votos, entre otros.
- Acciones estratégicas: sistemas de información clave para el Gobierno Vasco que tienen un papel relevante en relación con las elecciones.
- Imagen institucional del Gobierno Vasco: acciones estratégicas del Gobierno Vasco encargados de proteger y preservar la imagen de la institución en todos los casos.
- Servicios informativos y de emergencias: esta agrupación incluye los activos que sustentan los principales canales y medios de comunicación del Gobierno Vasco, así como los servicios de Emergencias de la población..

4 Fases a cubrir

Para garantizar los objetivos anteriores, el operativo se ha dividido en tres fases diferenciadas.

4.1 Etapa de preparación

Comienza en el momento de la adjudicación. En esta fase se deben diseñar y ejecutar al menos las siguientes acciones para mitigar los riesgos detectados:

- Identificación de qué se quiere monitorizar. Debe incluir al menos:
 - a. Direcciones IP y dominios
 - i. Nuevas resoluciones IP-dominio
 - ii. Nuevos subdominios
 - iii. Certificados expedidos
 - iv. Tecnologías empleadas
 - v. Puestos expuestos
 - vi. Cambio en los registros DNS
 - b. Darknet y leaks
 - i. Menciones en redes sociales
 - ii. Menciones en foros underground
 - iii. Menciones de actores APT y ciberdelinquentes
 - iv. Venta de credenciales en mercado negro
 - v. Credenciales expuestas en Internet
 - vi. Direcciones de email de VIPs que figuren en brechas
 - vii. Contenido subido a plataformas malware que esté relacionado
 - c. Otros
 - i. Búsqueda de versiones web en históricos
 - ii. Creación de dominios similares al original
 - iii. Correos de phishing relacionados con el evento
 - iv. Ataques contra AAPP relacionados con el evento
- Social Listening Tools
 - a. Elegir y desplegar las herramientas más apropiadas
 - b. Elegir los principales data feeds (Twitter, Youtube, news, foros, blogs, etc.)
 - c. Detección OSINT en tiempo real
- Diseño y preparación de herramienta deception que simule la web oficial de publicación de los resultados electorales. Los objetivos son:
 - a. Facilitar la detección temprana de ataques dirigidos a la organización en fase de reconocimiento
 - b. Obtener en el proceso Indicadores de Compromiso (IOCs) únicos y dirigidos a Ejie o al Gobierno Vasco
 - c. Identificar Técnicas, Tácticas y Procedimientos con base en el conocimiento disponible en MITRE ATT&CK, que nos llevará a la identificación plausible de los autores de los ataques
 - d. Conseguir comprometer a los adversarios en la infraestructura de Deception mediante la definición de Attack Paths, con el fin de mantenerles apartados de los activos reales y obtener la mayor cantidad de información posible del ataque mediante desafíos y astutas trampas que confundan y reten al atacante de manera dinámica y eficiente
 - e. Descubrimiento y análisis de actores y ciberamenazas previamente no identificadas

- f. Obtener inteligencia que permita realizar acciones orientadas al alineamiento de la estrategia corporativa de seguridad y los recursos disponibles con una postura de seguridad más eficiente
- Recopilación y análisis de datos (Bigdata): normalización de los datos y visualización mediante dashboards
- Definición de puntos de contacto: tarea conjunta entre el licitante y el adjudicatario que consistirá en identificar los puntos de contacto a los que reportar cualquier actividad maliciosa identificada.

4.2 Etapa de activación

Comienza en el momento que se anuncien las elecciones (54 días antes de la jornada electoral). Fase de activación del servicio de monitorización y análisis de ciberamenazas, con seguimiento de actores relevantes de ciberamenaza, contextos emergentes y observación de la superficie de exposición de los sistemas informáticos y redes de comunicaciones a proteger. Incluye:

- Prevención y respuesta ante ciberataques
- Obtención de datos estadísticos y tendencias
 - Identificación de fechas relevantes (debates, eventos, etc.).
 - Análisis temático
- Modelado de comportamientos de perfiles falsos y bots
- Contenido generado por IA
 - Imágenes falsas
 - Videos falsos

Se desplegará y operará la herramienta deception que simule la web oficial de publicación de los resultados electorales preparada en la fase anterior.

Alerta temprana: en el caso de identificar actividad maliciosa se procederá a su inmediata notificación a los puntos de contacto definidos. Se pondrá a disposición del adjudicatario una cuenta de correo desde la que centralizará todas las comunicaciones.

4.3 Etapa posterior a la jornada electoral

Una vez concluya el operativo, el adjudicatario del servicio presentará un informe final que recoja toda la actividad analizada durante el periodo del operativo, así como las conclusiones extraídas a partir de la misma.

5 Requisitos tecnológicos

5.1 Capacidades de la plataforma de deception

La plataforma de deception a desplegar deberá cubrir, al menos, las siguientes capacidades:

- Se debe desplegar una solución de decepción o engaño que esté activa por el tiempo de duración del contrato
- La plataforma de engaño debe ser modular y permitir el despliegue de los nodos que sean necesarios para poder cubrir los objetivos del escenario diseñado
- La arquitectura de la plataforma debe consistir en un orquestador de campañas, un conjunto de colectores y concentradores de información, un conjunto de nodos de engaño o deception donde se monitoriza la actividad y un conjunto de activos de engaño, cebos o señuelos
- En los nodos de deception los agentes desplegados deben operar al nivel de kernel y monitorizar comportamientos tanto a nivel de usuario como a nivel de sistema
- Los nodos concentradores deben aislar el entorno de engaño de la red de gestión de la plataforma donde se encuentra el orquestador
- La plataforma de engaño debe permitir la gestión desde una consola web centralizada de toda la infraestructura y de las campañas de engaño desplegadas
- La herramienta debe permitir simular una web oficial alojada en una nube pública
- Debe facilitar la detección temprana de ataques dirigidos a la organización en la fase de reconocimiento
- El orquestador debe permitir el diseño de campañas y la configuración de activos de engaño de manera instrumentalizada y mediante una interfaz web
- Debe permitir el despliegue de señuelos de información en múltiples formatos (ficheros, bases de datos, cuentas) y sistemas informáticos cebo (servidores, redes)
- La plataforma debe permitir la simulación de actividad real de usuarios mediante mecanismos de machine learning
- Debe permitir el seguimiento en tiempo real de la actividad maliciosa que realicen los posibles atacantes sobre los señuelos
- Debe facilitar la función de threat hunting o caza de amenazas, asegurando que todas las trazas digitales generadas por los activos de engaño estén disponibles para un análisis más exhaustivo y proporcionando una interfaz gráfica que permita visualizar la actividad maliciosa
- Debe permitir la obtención de Indicadores de Compromiso únicos y poder ser dirigidos a Ejie o al Gobierno Vasco a partir de la actividad maliciosa
- Debe permitir la identificación de las Técnicas, Tácticas y Procedimientos de acuerdo con el marco MITRE ATT&CK para poder asociar la actividad maliciosa a los posibles atacantes
- Debe facilitar mecanismos para atraer a los posibles atacantes sobre la red de señuelos, que debe ser lo suficientemente creíble para asegurar que mantengan su actividad sobre esa red y no accedan a la red de activos reales
- Los agentes desplegados en los nodos de engaño deben estar camuflados y utilizar canales ocultos seguros para comunicar su actividad a los nodos concentradores
- La plataforma debe poder adaptarse al comportamiento del adversario de manera automática
- Debe permitir obtener la mayor cantidad de información posible del ataque mediante desafíos y astutas trampas que confundan y reten al atacante de manera dinámica y eficiente

- Debe permitir el descubrimiento y análisis de actores y ciberamenazas previamente no identificadas
- La plataforma debe permitir el envío de alertas ante una detección, notificándolas automáticamente a un SOC vía SMTP, vía SYSLOG; por correo; o utilizando aplicaciones de mensajería como SIGNAL, SLACK, SYSLOG, MS TEAMS o TELEGRAM.
- La plataforma debe facilitar el análisis de malware analizando cualquier binario con VirusTotal y Reglas YARA o enviándolo automáticamente a un Sandbox CUCKOO existente
- Debe permitir la generación de informes en formato html y pdf

6 Entregables

Se establecen los siguientes hitos en el proyecto:

- Desde la puesta en marcha de la plataforma deception, elaboración y difusión de **Informes Semanales de Actividad**. En caso de actividad de especial relevancia, se podrá reducir la periodicidad.
- 30 días antes de la jornada electoral: elaboración y difusión de un **Informe de Perspectiva de Ciberamenazas** sobre el evento, con un análisis prospectivo de escenarios de posibilidad y recomendaciones de ciberseguridad preventiva.
- 15 días antes de la jornada electoral: elaboración y difusión de dos **Informes Semanales de Actualización** sobre actores ciberamenazas y nuevas vulnerabilidades relevantes para la superficie de exposición.
- Semana previa a la jornada electoral: elaboración y difusión de **Informes Diarios de Actualización** sobre actores de ciberamenazas y nuevas vulnerabilidades relevantes para la superficie de exposición.
- Posterior a la jornada electoral: **informe de conclusiones y oportunidades de mejora**

Durante la jornada electoral se deberá notificar de forma inmediata cualquier incidencia o actividad maliciosa.