BANCO DE INNOVACIÓN EN LAS ADMINISTRACIONES PÚBLICAS

TÍTULO

La Diputación de Cádiz implanta un Sistema de Información de Seguridad y Administración de Eventos

INFORMACIÓN INICIAL:

PROBLEMA:

El acceso público a la red DMZ (del inglés DeMilitarized Zone, Aunque su uso es habitual en redes de grande empresas creando una zona segura de acceso a determinados equipos que se encuentran separados de otros) de la Diputación de Cádiz puede provocar que dicha red sufra ataques informáticos de cualquier parte del mundo, por lo que es una red con alta prioridad para ser monitorizada. De igual modo, las conexiones establecidas a Internet por trabajadores internos de la Diputación de Cádiz también pueden provocar ataques informáticos, por lo que dichas conexiones también deben ser monitorizadas. Como respuesta avanzada se crea el sistema de seguridad y administración de eventos en la red corporativa.

SOLUCIÓN GLOBAL:

La Diputación Provincial de Cádiz dispone de una Red Corporativa Provincial de telecomunicaciones, suministrada por un operador de telecomunicaciones, que proporciona servicio de datos y voz a todas las dependencias de la Diputación, sus organismos autónomos y entidades locales a los que da servicio.

Borde de la organización

La infraestructura de borde de la organización agrupa la conectividad de varios dispositivos externos al campus de la organización y dirige el tráfico hacia la capa de núcleo de la infraestructura de red interna. Los módulos pertenecientes al área de borde de la organización ofrecen funcionalidades de seguridad que defienden los recursos de la organización cuando se producen conexiones con redes públicas y/o Internet. La topología lógica del área de borde de la organización incluye el extremo del ISP y el área remota.

Alcance

Este proyecto se aplica a la definición e implantación de un sistema de información de seguridad y administración de eventos en la red interna de la Diputación Provincial de Cádiz.

COSTE APROXIMADO:

Aunque resulta difícil realizar una estimación, al pertenecer la empresa a la corporación y ser su finalidad

surtir de servicios necesarios para ello, usándose adicionalmente un software abierto lo que no incrementa los costes de implantación o creación, se puede afirmar, por lo tanto, que se ha desarrollado con medios propios

TERRITORIO:

PROVINCIA DE CÁDIZ, comprendiendo a la Diputación, Organismos Autónomos y entidades locales.

PÚBLICO DESTINATARIO:

El público destinatario de este servicio es la generalidad de las interrelaciones con la administración por vía de la red corporativa de telecomunicaciones, al tratarse de un servicio de implementación de la seguridad de las redes.

ENTIDAD QUE LA HA LLEVADO A CABO:

La entidad responsable del desarrollo e implantación ha recaído sobre el Diputación de Provincial de Cádiz, más concretamente, por mediación de la Empresa Provincial de Información de Cádiz, S.A. (EPICSA). Se trata de una empresa pública creada en 1984 por la Diputación de Cádiz con el objeto social de dar asistencia técnica informática integral, formación, comercialización y desarrollo, así como implantación de aplicaciones informáticas, tanto a la propia Diputación como a sus organismos, empresas y municipios de menos de 20.000 habitantes.

DESCRIPCIÓN DE LA POLÍTICA O PROGRAMA:

Descripción de la solución propuesta, Solución software:

La red provincial de la Diputación de Cádiz, la cual gestiona EPICSA, engloba un gran número de activos. Es una red con muchos activos de diferente tipología (equipos personales, servidores, impresoras, etc., que generan una gran cantidad de tráfico de diferente tipo (TCP, ICMP, ARP, etc.).

Si se realiza un cálculo del máximo de activos a monitorizar que la red podría poseer en un momento determinado, la red de la Diputación de Cádiz proporciona conexión a 18 sedes de esta entidad, lo que se traduce en 23 bloques de direcciones IP, con máscara de subred de 24 bits, es decir, subredes de clase C, que pueden albergar, como máximo, 254 equipos a la vez. La red desmilitarizada, con sede en EPICSA, posee un bloque de direcciones IP clase C. La red de servidores tiene asignada un bloque de direcciones IP con máscara de subred de 19 bits, lo que se traduce en 8.180 activos, como máximo.

(24 Redes C * 254 Activos/Red C) + (1 Red de máscara 19 * 8180 Activos/Red) = 14.276 activos.

En el peor caso posible, la red de la Diputación de Cádiz estaría soportando el tráfico de red de 14.276 activos, que sería el mismo número de activos a monitorizar por el SIEM (Security Information Event Management). Este es el factor más determinante a la hora de seleccionar un SIEM, ya que, todos los SIEMs que ofrecen licencias limitadas a un cierto número de activos a monitorizar, no se acercan a la cifra de activos posibles de la red de la Diputación de Cádiz.

El SIEM que se vaya a desplegar en la red de la Diputación de Cádiz debe ser lo suficientemente versátil como para soportar la gran cantidad de activos presentes en la red, así como la variedad de tráfico que se va a monitorizar. Por ello, el software elegido es OSSIM, ya que es de código abierto y no ofrece ningún tipo de limitación en lo referente a licencias ni número de activos a monitorizar y, si el hardware sobre el que OSSIM está instalado posee la suficiente capacidad, la escalabilidad de OSSIM es muy considerable.

Localización de los sensores

Para que el sistema OSSIM que se va a desplegar en la red de la Diputación de Cádiz detecte todos los posibles ataques que se lleven a cabo, es necesario que dicho sistema OSSIM tenga la máxima visibilidad posible de todo el tráfico que se desea monitorizar. Para conseguir toda la visibilidad del tráfico y de los activos de la red de la Diputación de Cádiz, se deben desplegar cuántos sensores sean necesarios. Según lo establecido en el requisito R-01, la zona prioritaria de monitorización es la zona frontera de la red.

En la zona frontera de la red de la Diputación de Cádiz aparecen diferentes tipos de conexiones:

- VPN sitio a sitio con el Ayto. de Puerto Real.
- VPNs sitio a sitio con las sedes remotas de la Diputación de Cádiz y Ayuntamientos de la provincia de Cádiz, de municipios de menos de 20.000 habitantes.
- VPN sitio a sitio con la sede SS.CC de la Diputación de Cádiz.
- VPNs de acceso remoto para teletrabajadores de la Diputación de Cádiz.
- Acceso público a la red DMZ mediante direccionamiento IP proporcionado por RIPE.
- Conexiones a Internet de trabajadores de las sedes de la Diputación de Cádiz pertenecientes al anillo de red metropolitano.

Todas las conexiones VPN anteriormente expuestas que se establecen en la red de la Diputación de Cádiz son conexiones conocidas, es decir, los usuarios que la utilizan son usuarios conocidos y, a priori, son conexiones que no van a generar tráfico malicioso, por lo que no son prioridad para ser monitorizadas.

El acceso público a la red DMZ de la Diputación de Cádiz puede provocar que dicha red sufra ataques informáticos de cualquier parte del mundo, por lo que es una red con alta prioridad para ser monitorizada. De igual modo, las conexiones establecidas a Internet por trabajadores internos de la Diputación de Cádiz

también pueden provocar ataques informáticos, por lo que dichas conexiones también deben ser monitorizadas.

A partir de ahora, el desarrollo de este apartado se va a centrar en los módulos de la zona frontera de la red de la Diputación de Cádiz denominados PRESENCIA EN INTERNET y CONECTIVIDAD A INTERNET, por lo que el esquema de red de la zona frontera de la red de la Diputación de Cádiz se verá simplificado.

En primer lugar, vamos a analizar las diferentes procedencias que un posible ataque informático podría tener en estos módulos de la zona frontera de la red de la Diputación de Cádiz.

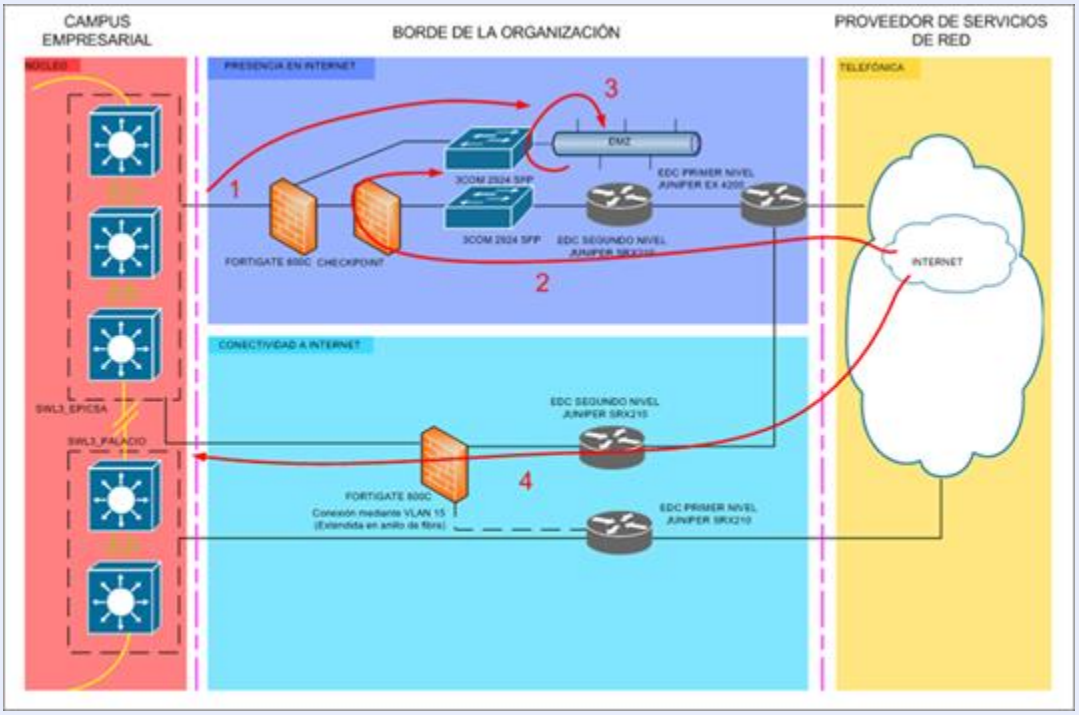

Figura 1. Módulos de la zona frontera.

Los orígenes de los posibles ataques a la zona frontera de la red de la Diputación de Cádiz son los siguientes:

- Ataque 1: Ataque interno a la red DMZ, ya sea por un virus en expansión en la red interna, por un usuario conocido con malas intenciones o por un atacante con acceso a la red interna.
- Ataque 2: Ataque externo a la red DMZ procedente de Internet.
- Ataque 3: Ataques entre propios activos de la red DMZ, ya sea por un virus en expansión en la red DMZ, por un usuario conocido con malas intenciones o por un atacante con acceso con privilegios a un activo de la red DMZ.
- Ataque 4: Ataque externo a la red interna procedente de internet debido a una conexión preestablecida por un usuario interno, por ejemplo, acceso a una web maliciosa, descarga de un ejecutable infectado, etc.

A modo de resumen, la procedencia y objetivo de esos ataques se puede observar en la siguiente tabla.

Ataque	Procedencia	Objetivo
1	LAN	DMZ
2	Internet	DMZ
3	DMZ	DMZ
4	Internet	LAN

T

Tabla 1. Orígenes de ataques a la zona frontera.

La localización de los sensores OSSIM a desplegar en la red de la Diputación de Cádiz debe asegurar que todo el tráfico de red generado por la aparición de alguno de los ataques expuestos anteriormente es monitorizado, por ello, la localización de los sensores OSSIM en la zona frontera de la red de la Diputación de Cádiz es la siguiente:

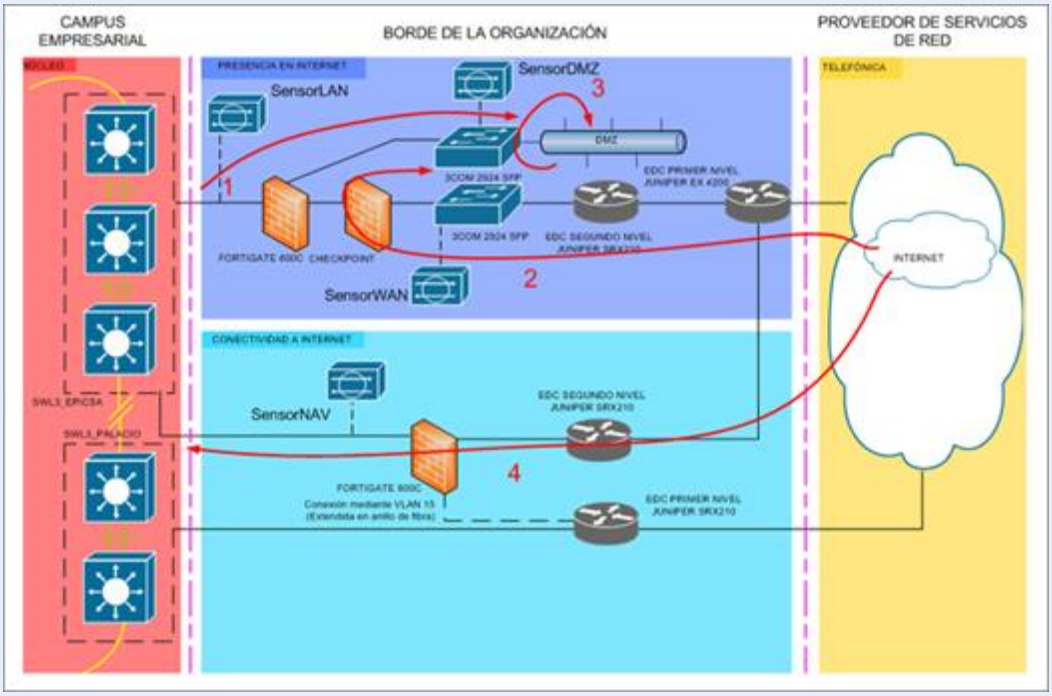

Figura 2. Localización de los sensores OSSIM en la zona frontera.

Es necesario que los sensores desplegados en la zona frontera de la red de la Diputación de Cádiz sean capaces de monitorizar todo el tráfico que transita la red para asegurar la correcta detección de ataques. Para ello, se realizarán las siguientes acciones, según el sensor desplegado.

- SensorLAN (detección de ataque 1). Se configura un puerto espejo en el clúster de conmutadores de núcleo, que refleje todos los puertos de dicho clúster conectados al clúster de cortafuegos Fortigate 600C.
- SensorWAN (detección de ataque 2). Se configura un puerto espejo en el conmutador externo que

refleja todo el tráfico entrante al clúster de cortafuegos Checkpoint.

- SensorDMZ (detección de ataque 3). Se configura un puerto espejo en el conmutador de la DMZ que refleje todos los puertos de conexión de servidores en la DMZ y los puertos de conexión al clúster de cortafuegos Fortigate 600C.
- SensorNAV (detección de ataque 4). Se configura un puerto espejo en el clúster de conmutadores HP 5500 de núcleo, que refleje los puertos de conexión del clúster de cortafuegos Fortigate 800C.

Con el despliegue de sensores expuesto anteriormente, se consigue monitorizar los módulos de la zona frontera de la red de la Diputación de Cádiz que más propensos son a sufrir un ataque y que, por tanto, tienen más prioridad en este proyecto.

Análisis de vulnerabilidades

Se estableció el requisito R-02, consistente en que el sistema OSSIM debe alertar sobre las vulnerabilidades encontradas en los activos de la red de la Diputación de Cádiz.

Debido al alto número de activos presentes en la red de la Diputación de Cádiz, los análisis de vulnerabilidades se realizarán a través de la red y, para conseguir la visibilidad máxima de todas las posibles vulnerabilidades de los equipos, todos los escáneres poseerán credenciales de administradores de los activos Windows de la Diputación de Cádiz, por lo que dichos escáneres se realizarán con perspectiva de administrador.

El sistema OSSIM debe analizar las vulnerabilidades en los activos presentes en todas y cada una de las subredes de la Diputación de Cádiz que se están monitorizando:

- Subredes clase C pertenecientes a las sedes de la Diputación de Cádiz pertenecientes al anillo de red metropolitano.
- Subred clase C perteneciente a la red DMZ de la Diputación de Cádiz.

Además, se configurará un escáner de vulnerabilidades en la red de servidores internos de EPICSA, cuyos activos se encuentran en los bloques de direcciones 172.22.8.0/24 y 172.22.9.0/24, respectivamente. Para controlar las vulnerabilidades que puedan aparecer en los dispositivos de red, se realizará un escáner de vulnerabilidades de la red de gestión de conmutadores del anillo de red metropolitano de la Diputación de Cádiz, cuya subred es la 172.32.1.0/24. Cada semana se repetirán todos los escáneres debido al alto grado de vulnerabilidades que aparecen semanalmente, de tal manera que la información sobre las vulnerabilidades presentas y/o vulnerabilidades a buscar sea la más actualizada posible. OpenVAS actualiza diariamente su base de vulnerabilidades y análisis de diversas fuentes como CVE (Common Vulnerabilities and Exposures).

La planificación semanal de los escáneres de vulnerabilidades se ha configurado de tal manera que nunca

coincidan temporalmente dos escáneres de vulnerabilidades, debido al alto nivel de tráfico que generan dichos escáneres.

Sensores:	DMZ	WAN	LAN	NAV		
Día / Hora	Lunes	Martes	Miércoles	Jueves	Viernes	Sábado	Domingo
8:00 -- 9:00							
9:00 -- 10:00	EPICSA PB	RESIDENCIA	PALACIO 1	PALACIO 3	EUROPA		
10:00 -- 11:00	EPICSA T	IEDT	PALACIO 2	PALACIO 4	RIVADAVIA		
11:00 -- 12:00	EPICSA PP	S. ANTONIO	ROMA	CAPUCHINOS	GLORIETA		
12:00 -- 13:00	EPICSA AF	ANTONIO L.	GUADAL.	AG. ENER.	MEDIA MB		
13:00 -- 14:00							
14:00 -- 15:00							
15:00 -- 16:00							
16:00 -- 17:00					Servidores 8	ANILLO	
17:00 -- 18:00					Servidores 9	DMZ	
18:00 -- 19:00							
19:00 -- 20:00							
20:00 -- 21:00							

Tabla II. Planificación semanal de los escáneres de vulnerabilidades.

Detección de intrusiones en red (NIDS)

El sistema OSSIM utiliza un detector de intrusiones en red llamado Suricata. Dicho sistema de detección de intrusiones en red utiliza un perfil de malo conocido para detectar ataques, ya que contiene almacenadas un conjunto de reglas que contrasta contra el tráfico que monitoriza para detectar patrones conocidos de ataques.

Suricata se ajusta a la perfección a la red de la Diputación de Cádiz, ya que su arquitectura está implementada de tal manera que soporte grandes cantidades de tráfico a analizar, debido a que soporta procesamiento multi-hilo. Las reglas que utiliza Suricata para detectar patrones de ataques se mantienen actualizadas diariamente por AlienVault y provienen de fuentes como la propia empresa y la comunidad Emerging Threats.

Por defecto, al desplegar el sistema OSSIM en un sensor que va a monitorizar tráfico de red, Suricata está activado por defecto en la interfaz que se configure como interfaz de monitorización. En el servidor OSSIM

desplegado en la red de la Diputación de Cádiz, toda la información relacionada con los eventos de seguridad detectados por Suricata se encuentra en Analysis > Security Events (SIEM).

En esta sección podemos visualizar todos los eventos generados por las diferentes fuentes de OSSIM, Suricata entre ellas, así como realizar búsquedas avanzadas y filtrar la información. En esta página principal encontramos información importante sobre los eventos: Nombre del evento, Fecha de origen, Sensor que lo ha generado, Relación con AlienVault OTX, Origen del evento, Destino del evento, Valor de importancia de los activos de origen y destino, Riesgo del evento.

Si pulsamos en un evento, podemos visualizar información más concreta sobre el mismo, así como el paquete de red que ha generado la alerta y la regla de Suricata que lo ha detectado. El sistema OSSIM también nos ofrece la posibilidad de descargar dicho paquete en formato PCAP por si se desea analizar con una herramienta más especializada, como Wireshark, por ejemplo.

En definitiva, con este sistema, se añade un elemento más en la seguridad de nuestra red, dando un paso más hacia el cumplimiento del Esquema Nacional de Seguridad, con la detección de intrusión y así identificar cualquier acceso sospechoso o no autorizado.

OBSTÁCULOS SUPERADOS:

El módulo de conectividad a Internet está constituido de la siguiente manera. Para la navegación a Internet de los empleados de la Diputación de Cádiz y de los ayuntamientos a los que EPICSA presta servicio, se ha desplegado un clúster de dos firewalls Fortigate 800C que gestiona las conexiones WAN con el ISP. Se han configurado dos rutas diferenciadas para el acceso a Internet, una en EPICSA y otra en la sede de Palacio. La conexión de Palacio al clúster de firewalls Fortigate 800C, que está físicamente situado en EPICSA, se realiza mediante una extensión lógica a través de la VLAN 15 (Fortigate), extendida en el anillo metropolitano. El clúster de firewalls Fortigate800C se encarga de balancear el tráfico de red del módulo de conectividad a internet entre las dos rutas configuradas en la red de la Diputación de Cádiz: EPICSA y Palacio Provincial. Así, pues, el obstáculo a superar ha sido la compatibilización del nuevo sistema de seguridad con los elementos de servicio existentes sin que existan alteraciones del sistema y de los servicios existentes.

IMPACTO:

En definitiva, con este sistema, se añade un elemento más en la seguridad de la red de la Diputación, dando

un paso más hacia el cumplimiento del Esquema Nacional de Seguridad, con la detección de intrusión y así identificar cualquier acceso sospechoso o no autorizado.

Premios:

- Premio Congreso Nacional de Innovación y Servicios Públicos, CNIS 2018

Premio proyecto consolidado de gestión de la seguridad al sistema de información de seguridad y administración de eventos en la red corporativa. Diputación Provincial de Cádiz

CALENDARIO DE IMPLANTACIÓN Y REFERENCIA TEMPORAL:

Proceso de implantación:

Desde su aprobación, la implantación del sistema se ha desarrollado en menos de un año.

DOCUMENTACIÓN DE CONSULTA Y APOYO:

Concesión premio:

https://www.clubdeinnovacion.es/los-premios-cnis-reflejan-alto-compromiso-los-responsables-publicos-la-transformacion-digital/

Documentos:

https://www.esmartcity.es/comunicaciones/comunicacion-sistema-monitorizacion-servicios-publicos-digitales-diputacion-de-cadiz