



TITULO DE LA OPERACIÓN:

SUMINISTRO DE UNA SOLUCIÓN DE SEGURIDAD DE APLICACIONES WEB, PARA LA RED DE COMUNICACIONES DE LA ADMINISTRACIÓN DEL PRINCIPADO DE ASTURIAS (expediente 23/2016)

DATOS PRINCIPALES:

Coste de la operación: 180.290 €

Cofinanciación FEDER: 80 %

BREVE DESCRIPCIÓN DEL PROYECTO

La Administración del Principado de Asturias ha venido realizando importantes avances en lo referido al mejor uso de las tecnologías de la información y las comunicaciones, tanto para su gestión interna como respuesta a las crecientes demandas de la ciudadanía en lo tocante a la llamada “administración electrónica”. El crecimiento en nuestras redes, en las demandas de conexión y acceso a las mismas, el aumento de uso de aplicaciones WEB, tanto interno como para el/la ciudadano/a, obliga a implementar medidas de protección y seguridad que impidan el éxito del también creciente número de ataques

En el caso concreto de aplicaciones web, que en su construcción primaron más la eficiencia en la entrega que la seguridad, nos encontramos con multitud de peligros y vulnerabilidades susceptibles de ser aprovechadas por potenciales atacantes.

Estas aplicaciones web requieren por lo tanto una protección adecuada basada en nuevos dispositivos surgidos ad-hoc para salvar las deficiencias que presentan otros sistemas más generalistas de protección como los cortafuegos tradicionales o los IPS (Sistema de prevención de intrusiones). Estos dispositivos específicos, los llamados WAF (Web Application Firewall o cortafuegos de aplicaciones web), son los contratados en el proyecto que nos ocupa y tienen una óptima capacidad para inspeccionar y filtrar tráfico web, realizando un análisis inteligente basado en evidencias pero también sospechas de por dónde y qué forma puede estar intentando realizarse un ataque.

OBJETIVOS Y RESULTADOS PREVISTOS

El objetivo final ha sido implantar una solución de seguridad en alta disponibilidad formada por dos máquinas cortafuegos de aplicaciones web, complementadas con una máquina para el estudio de evidencias sospechosas dentro de un entorno controlado denominado Sandbox, y todas ellas destinadas a detectar y bloquear intentos de entrada de ataques que aprovechan la debilidad o vulnerabilidades de aplicaciones WEB, ataques dirigidos tanto a perjudicar el uso de esas aplicaciones como a penetrar en el resto de redes del Principado usando esa puerta de acceso que han logrado a través de una aplicación insegura.