CONVOCATORIA DE PREMIOS @asLAN

A PROYECTOS DE TRANSFORMACIÓN DIGITAL EN ADMINISTRACIONES

Y ORGANISMOS PÚBLICOS

EL OSO Y ELGOLEM. EVALUACIÓN Y DESPLIEGUE DE UN SISTEMA AVANZADO DE PROTECCIÓN Y RECOLECCIÓN DE DATOS EN ESTACIONES DE TRABAJO.

Implantado en: Gobierno de Navarra

Nafarroako Gobernua
Gobierno de Navarra

panda

ANTECEDENTES/PROBLEMÁTICA

Gobierno de Navarra gestiona unas 12.000 estaciones de trabajo situadas en más de 400 localizaciones diferentes a lo largo y ancho de la geografía de Navarra con una gran heterogeneidad de entornos y software instalado.

Cuando Microsoft dejó de dar soporte a su sistema operativo Windows XP en el año 2014, la migración a otros nuevos estándares era minoritaria e iba a tardar en completarse por motivos técnicos y organizativos. El hecho de que un porcentaje significativo de equipos no recibieran actualizaciones de seguridad por un periodo de tiempo indeterminado suponía un riesgo inaceptable.

Al mismo tiempo, se hacía patente para el equipo de Seguridad que el entorno de cyberamenazas obligaba a tomar medidas avanzadas de protección a nivel de puesto de trabajo. El tiempo cada vez más breve entre el descubrimiento de un agujero de seguridad y su explotación con fines maliciosos (exploits), el ritmo de actualizaciones vertiginoso (flash, java, Microsoft,…), el auge del ransomware, las técnicas de ocultación de tráfico etc. hacían que los sistemas antimalware tradicionales o las soluciones perimetrales resultaran insuficientes.

Por todo ello, Gobierno de Navarra decidió evolucionar su plataforma antimalware de puesto de trabajo.

OBJETIVOS PERSEGUIDOS

Para este proyecto se persiguieron dos objetivos:

- Incrementar la seguridad del puesto de trabajo mediante una capa de protección adicional a los parches de seguridad que proporcionan los fabricantes de software durante la vida útil de sus productos.

- Añadir una capa de protección adicional a los antivirus tradicionales basados en firmas, cadenas de código y nombres de ejecutables.

Funcionalidad requerida del producto:

- Ser una solución local para puestos de trabajo, que los proteja tanto en el interior como en el exterior de la red corporativa.
- Bloquear la ejecución de malware incluyendo vulnerabilidades del tipo 'día cero' (0-day's) sin parche publicado.
- Funcionar de un modo complementario a las firmas de los antivirus o control de red, monitorizando el comportamiento en el puesto.
- Alertar de los intentos de uso malicioso.
- Dejar un registro de los mismos.
- Ser gestionable de manera centralizada por parte de los distintos grupos de soporte técnico de Gobierno de Navarra.
- Demostrar un impacto mínimo en el rendimiento del puesto, y que sea válida para equipos *legacy*.
- Ofrecer servicios profesionales y de mantenimiento avanzados a través de sus proveedores.

Evidentemente, todo debía llevarse a cabo con un coste asumible.

FASES DEL PROYECTO – RECURSOS EMPLEADOS

Evaluación

En primer lugar, se realizó un análisis de mercado, del que se seleccionaron varios productos. A continuación se procedió a la evaluación de las funcionalidades y eficacia de los mismos mediante pruebas en dos tipos de entornos:

- en un entorno controlado de laboratorio con equipos virtuales XP (con y sin parches) y Windows 7 (con y sin parches) y con conexión directa a internet, es decir, sin protección perimetral.
- en un despliegue piloto sobre 200 máquinas reales, seleccionadas para que fueran representativas de la realidad de Gobierno de Navarra.

Las pruebas realizadas en laboratorio consistieron en la utilización de varias herramientas de "Exploit Test", el uso de malware recogido en incidencias reales en Gobierno de Navarra y pruebas de e-crime y auditoría.

Tras la evaluación de los resultados la solución elegida fue Panda Adaptive Defense 360. (PAD 360)

Despliegue

El despliegue se llevó a cabo en varias fases de forma controlada

- Fase piloto, realizada en dos partes con un primer despliegue limitado que fue ampliado posteriormente a un número de máquinas que se consideró significativo, incluyendo estaciones con Windows XP, Windows 7 y Servidores Citrix con Windows 2008 R2. Una vez comprobado que no existían problemas ni incompatibilidades con el software instalado se pasó a las siguientes fases.

- Fase de expansión, donde se amplió el despliegue de PAD 360 a 1.000 estaciones de trabajo más.

- Fase masiva, una vez comprobado que no existían grandes incompatibilidades, el despliegue se realiza a la totalidad de estaciones de trabajo y Servidores de Citrix.

En paralelo se acometen otras fases del proyecto relacionadas con la recogida de los datos que las estaciones con PAD 360 instalado envían al Cloud de Panda.

Integración con ELGoLEM

Una de las características del módulo de protección avanzada de PAD 360 es que suministra un constante flujo de información sobre todos los procesos que se ejecutan en las estaciones de trabajo, sobre los accesos y modificaciones en el registro de Windows y sobre las conexiones de red efectuadas. Los datos brutos se tratan en primera instancia por sistemas de clasificación automática que hacen uso de técnicas de "Machine Learning" en la plataforma Big Data de Panda.

Esta información es todo lo que necesita la solución para bloquear software malicioso y proteger los equipos. Sin embargo, en Gobierno de Navarra se apostó por explotar en profundidad la información recogida para conocer mejor la situación del parque y favorecer la toma de decisiones.

En primer lugar, se estableció un flujo de información a través de una conexión segura hasta un repositorio corporativo del CPD de Gobierno de Navarra. Dichos logs son recolectados por el SIEM Lookwise Enterprise Manager (LEM) de S21sec, que los normaliza y estructura para que sean consultables de manera sencilla por sentencias SQL. El volumen de datos recibido es de 12 GB diarios aproximadamente, previos a la compresión y son custodiados de manera segura y durante un periodo de retención ilimitado.

A partir de ese momento, la información puede explotarse a través de una plataforma de Big Data Security Analytics, basada en herramientas de código abierto, ELG, (ElasticSearch, LogTash y GrayLog), de donde deriva su nombre: ELGoLEM (ELG over LEM).

Dicha plataforma es capaz de cruzar y enriquecer la información contenida en log de PAD360, ya de por sí muy rico, con la de otras herramientas de seguridad, inventario, DA, y un largo etc. Ofreciendo la posibilidad de realizar análisis exhaustivos y completos del comportamiento de las máquinas del parque, convenientemente contextualizados para la operativa real, el análisis de situación y la toma de decisiones. Hay varios casos de uso que han resultado de gran interés, como la detección de máquinas

virtuales no controladas, detección de ataques “malware-free”, re-análisis automatizado en virus total o presencia de ejecutables de baja prevalencia, entre otros muchos.

Para las tareas referentes al correcto establecimiento de las conexiones entre los sistemas de Panda y Gobierno de Navarra, el volcado de la información y la interpretación de los datos suministrados se ha contado con el asesoramiento de los técnicos de Panda y de S21sec.

MEJORAS EN EFICIENCIA Y REDUCCIONES DE COSTE

Elevado nivel de protección

Los indicadores obtenidos tras el despliegue de PAD 360 nos ofrecen los siguientes datos:

- No se ha dado ninguna incidencia por infecciones de malware desde que se ha puesto PAD 360 en modo “hardening”.
- No se ha sufrido ninguna incidencia por ataque de ransomware en la que se hayan cifrado archivos.
- No se ha encontrado evidencia de que se haya intentado producir ataques malware-free (es decir, por powershell o equivalentes). Pero sí se han detectado dichos comportamientos cuando tuvieron lugar durante auditorías controladas.
- No se han detectado intentos de acceso a redes de Command & Control en el cortafuegos perimetral.

Mejoras en visibilidad sobre las estaciones

Es interesante constatar que, gracias a la solución, ahora disponemos de herramientas que nos dan visibilidad sobre las mismas por los que es posible realizar análisis de situación o análisis forenses en los que se puede llegar al nivel de detalle sobre qué “exploit” se está ejecutando en la máquina.

Gracias a todo esto, mediante la explotación de la información en ELGoLEM y generación de alertas altamente personalizadas en Lookwise EM, ha sido posible expandir el grado de control que se tiene sobre la red corporativa e incrementar el nivel de seguridad en la misma. Realizar los análisis que han culminado en dichas protección sin la información proporcionada por PAD 360 y las capacidades de explotación de ELGoLEM hubiese conllevado un esfuerzo desproporcionado o, directamente, irrealizable.

Reducción de costes

El hecho de no haber sufrido ninguna infección, hace pensar que el despliegue de PAD 360 ha supuesto un ahorro considerable en horas de técnicos del CAU, especialistas y usuarios. Este hecho es particularmente cierto en el caso del ransomware, que venía provocando numerosas incidencias desde el año 2015; algunas de las cuales supusieron horas de bloqueo a recursos compartidos, esfuerzos considerables de recuperación de datos y, en definitiva, pérdida de horas productivas para negocio y los equipos de soporte.

Cumplimiento normativo

Desde el punto de vista de cumplimiento normativo en Administraciones Públicas, los productos antimalware tradicionales basados en firmas nos permiten dar cumplimiento a algunas de las medidas de seguridad que exige el Esquema Nacional de Seguridad, como la **Protección frente a código dañino [op.exp.6] y la Protección del correo electrónico (email) [mp.s.1].**

Sin embargo, al contar con una solución de protección avanzada basada en análisis del comportamiento de los procesos, y con una herramienta de correlación de eventos y auditoría forense automatizada, podemos dar cumplimiento a medidas adicionales de difícil solución como la necesidad de registrar y analizar la actividad de los usuarios para identificar acciones indebidas o no autorizadas recogida en el **Artículo 23. Registro de actividad, y la medida de seguridad op.exp.8 Registro de actividad de los usuarios.**

Finalmente, el Esquema Nacional de Seguridad nos obliga a contratar productos de seguridad que cuenten con certificaciones reconocidas internacionalmente (**Artículo 18. Adquisición de productos de seguridad y contratación de servicios de seguridad, y medida de seguridad op.pl.5 Componentes certificados**). Siendo Common Criteria una de las más reconocidas mundialmente, este apartado quedará también plenamente cubierto.

CONCLUSIONES DE LA ENTIDAD

A la luz de los indicadores investigados, se concluye que la solución de protección antimalware PAD360 y su integración con ELGoLEM ha resultado muy beneficiosa para Gobierno de Navarra en los aspectos de:

- Mejora del nivel de protección del puesto dentro y fuera de la red corporativa, evidenciado en un descenso de incidencias de seguridad. Este hecho conlleva una menor dedicación de técnicos de soporte y especialistas, además de evitar la pérdida de horas productivas para equipos de negocio u otros impactos potenciales.
- Aunque no se cuantificado, es argumentable que por todas esas razones el Retorno de Inversión justifica los esfuerzos realizados.
- Se ha obtenido una mayor visibilidad sobre la actividad de las estaciones, lo cual posibilita interpretar con datos fiables y objetivos la realidad del parque de estaciones y tomar decisiones de índole técnica y organizativa para una mejor gestión de la seguridad.
- Mayor adecuación a los requerimientos establecidos por el ENS.