CONVOCATORIA DE PREMIOS @asLAN
A PROYECTOS EN LA ADMINISTRACIÓN PÚBLICA

LA VIDA DEL DATO EN EL MINISTERIO DE JUSTICIA: CONTROL EN EL PUNTO DE ACCESO Y PROTECCIÓN DE FUGAS

Implantado en:

GOBIERNO DE ESPAÑA MINISTERIO DE JUSTICIA dtic División de Tecnologías de la Información y las Comunicaciones

Symantec. FORTINET axians

ANTECEDENTES

En los últimos años, la protección del dato ha adquirido una importancia cada vez más crítica para la gestión adecuada de los sistemas de información. El desarrollo de las tecnologías de información y comunicaciones, junto con el uso de tecnologías móviles e inalámbricas, hace que los ciberataques supongan amenazas que es necesario gestionar, por lo que el Ministerio de Justicia ha desarrollado un proyecto de seguridad global que busca minimizar los riesgos y proteger los activos actuando en los distintos sistemas de información.

RETOS - OBJETIVOS PERSEGUIDOS

El objetivo del proyecto es actuar en los distintos sistemas y segmentos de red para proteger los datos, integrando a su vez la información de distintas fuentes para tener una visión global de lo que sucede en las infraestructuras del ministerio. Para ello se han implementado diversos proyectos en el ámbito de la seguridad que se describen a continuación.

FASES DEL PROYECTO – RECURSOS EMPLEADOS

Desde el año 2016 el Ministerio de Justicia ha ampliado la capacidad y las funcionalidades de sus distintos sistemas de seguridad, implantando además nuevos sistemas que permiten proteger el dato desde su creación hasta su acceso por parte de los usuarios.

Para todo ello, la DTIC ha contado con recursos internos y distintos colaboradores tecnológicos, destacando Symantec, Fortinet, Axians, Oesía, Indra, Telefónica, Alienvault, Cisco, Forescout, F5 Networks y el CCN.

Proyecto 1: Desarrollo de la normativa de seguridad

Como primer paso, imprescindible para aplicar las distintas medidas de seguridad, se ha desarrollado y aprobado la Política de Seguridad del Ministerio [*Orden JUS/1293/2017, de 14 de diciembre, por la que se aprueba la Política de Seguridad de la Información en el ámbito de la administración electrónica, BOE nº 315 de 28 de diciembre de 2017]* que establece las bases de la normativa posterior. Tras la aprobación de la política, se ha iniciado el desarrollo de normativas e instrucciones técnicas que detallen el uso de los recursos, destacando la *"Norma de utilización de los recursos y Sistemas de Información del Ministerio de Justicia*", que establece el uso de los recursos por parte de los usuarios, y habilita a los responsables de seguridad a tomar las acciones necesarias para velar por la seguridad de los datos, así como realizar una adecuada gestión de los incidentes.

Proyecto 2: Control de Acceso a Red

El Ministerio de Justicia ha implantado un NAC, basado en Forescout, que permite securizar el acceso a la red, permitiendo a la vez que dispositivos no corporativos accedan a determinados servicios siempre que cumplan determinadas condiciones. De esta manera, se puede garantizar que los equipos que acceden a la red tienen sistemas de antivirus, y las actualizaciones de sistema operativo, necesarias para impedir la intrusión y propagación de malware en la red interna del ministerio.

Se ha implantado también una nueva y mejorada VPN mediante F5 Big IP para el acceso a recursos internos desde la red externa del ministerio, securizando y controlando los accesos de los usuarios en función de las necesidades concretas.

Proyecto 3: Detección de malware: Navegación, puesto de usuario y correo electrónico

El Ministerio de Justicia cuenta con proxys Bluecoat que protegen la navegación de los usuarios en internet. Durante 2018 se han adquirido nuevos equipos con más potencia, para mejorar la capacidad de análisis de las conexiones. Como medida de protección adicional, se ha comenzado a usar el Content Malware Analysis (CAS) que analiza todas las descargas, haciendo uso de sandboxing, añadiendo una capa adicional de protección antimalware. Los resultados del análisis de las descargas en la Sandbox, pueden integrarse con el agente de los puestos de usuario, de manera que si se detecta un archivo potencialmente peligroso que esté presente en un equipo, el sistema de antivirus pueda tomar las medidas adecuadas.

A nivel de correo electrónico, se cuenta con un sistema de filtrado y antivirus de correo basado en Ironport, que permite el análisis y filtrado de la información cursada por las infraestructuras de datos para asegurar que no contiene amenazas. Esta información se complementa con las funcionalidades presentes en las distintas capas de cortafuegos, que al involucrar distintos fabricantes y fuentes de información permiten detectar un abanico más amplio de amenazas. La correlación de dicha información, aporta un nivel mayor de protección en los sistemas de correo.

Proyecto 4: Protección de las aplicaciones

Los servicios proporcionados por el Ministerio de Justicia, se encuentran protegidos por una doble barrera de cortafuegos de distintas tecnologías, alimentados con información de listas negras proporcionada por el Centro Criptológico Nacional a través de REYES. Los distintos servicios son sometidos a auditorias periódicas para minimizar las vulnerabilidades, pero estas medidas no son suficientes para conseguir una seguridad adecuada. Por ello, adicionalmente desde 2016 se ha trabajado en implantar un Web Application Firewall, Fortiweb, extendiendo la protección de los cortafuegos a la capa de aplicación. El WAF permite identificar el comportamiento estándar de los servicios, de manera que sea posible la detección de anomalías y la creación de filtros adaptados.

Proyecto 5: Prevención de pérdida de datos

Durante el año 2018, con el objetivo de controlar las posibles fugas de información, el Ministerio de Justicia ha adquirido una solución de "Data Loss Prevention" de Symantec, que permite auditar las acciones que se realizan sobre archivos que contienen información sensible, ubicados en carpetas compartidas o sitios de colaboración, en los que el acceso de varios usuarios puede suponer un riesgo de fuga de información. Esta información puede integrarse también con los sistemas de navegación, de forma que se consiga una visión global de la información, y con los antivirus de puestos de usuario, para extender la protección y aumentar la trazabilidad de los datos.

Proyecto 6: Centralización y correlación de logs

Durante el año 2018 el Ministerio de justicia ha trabajado en implantar una solución de centralización de logs, basada en Graylog que permite almacenar y gestionar la información generada por los distintos sistemas, de manera que faciliten el análisis ante incidentes.

Adicionalmente, se ha realizado la implantación Alienvault, un SIEM (Security Information and Event Management) que centraliza el almacenamiento y mejora la interpretación de los datos relevantes de seguridad, proporcionando una visión unificada de los logs de distintos sistemas, haciendo posible la detección de actividades anómalas y la trazabilidad de las actividades de los usuarios. De esta manera, se puede realizar una monitorización y correlación de los datos en tiempo real.

Proyecto 7: Servicio de vigilancia digital

El Servicio de Vigilancia Digital con el que cuenta el Ministerio desde el año 2018, proporcionado por OESIA consiste en un servicio de cibervigilancia digital en Internet para la identificación de riesgos potenciales derivados de las nuevas amenazas digitales. Este servicio permite al ministerio:

- Detección proactiva de ataques para activar medidas de seguridad que los mitiguen
- Minimizar los riesgos de suplantación de identidad, robo de credenciales, incumplimientos legales, fugas de información, hacktivismo, ataques DDoS o vulneración de mecanismos de seguridad.
- Evaluación de la imagen de la institución en usuarios de internet.

El servicio permitirá la explotación de datos recogidos relacionados con el Ministerio de Justicia en "Fuentes abiertas", que incluyen redes sociales, foros, blogs, noticias, etc. Estas fuentes contienen información accesible por cualquier persona o entidad y no son de carácter clasificado. Por otra parte, se contempla en el servicio el rastreo de información en la "Deep Web".

Proyecto 8: Campaña de Concienciación

En una estrategia global de ciberseguridad, es necesario implicar a los usuarios, frecuentemente considerados el eslabón más débil de la seguridad informática. Por ello, el Ministerio de Justicia inició en 2017 una campaña de concienciación como medida para minimizar los ataques por ingeniería social, reforzando la participación de los usuarios en las medidas de seguridad adoptadas. En el marco de la campaña se ha elaborado cartelería para las dependencias del ministerio, y se han realizado envíos de correo con noticias de actualidad y consejos de seguridad.

NUEVOS SERVICIOS, MEJORAS EN EFICIENCIA Y REDUCCIONES DE COSTE

Mediante la ejecución de los proyectos anteriores, el Ministerio de Justicia ha extendido la protección de los datos en distintos niveles:

- Desarrollo de la normativa de seguridad, estableciendo el uso de los recursos proporcionados a los usuarios y definiendo el marco de las actuaciones de ciberseguridad.
- Control de acceso a la red de dispositivos corporativos y externo mediante tecnologías NAC y VPN.
- Detección y protección ante malware, destacando:
    - Análisis en tiempo real de las descargas de los usuarios con CAS y ejecución en Sandbox.
    - Análisis en tiempo real de correo electrónico.
    - Protección de los PCs de usuarios.
- Protección de ciberataques nivel de aplicación mediante firewalls de red y de aplicaciones.
- Protección de la información sensible ante accesos no autorizados y control de posibles fugas de información mediante el DLP.
- Análisis de la información disponible en las distintas fuentes mediante el SIEM.
- Servicio de vigilancia digital proactiva que permita anticiparse a posibles incidentes de seguridad.

- Concienciación de los usuarios, reforzando el que se considera el eslabón más débil de la seguridad informática.

Estos elementos permiten al Ministerio de Justicia contar con la protección de los datos a lo largo de todo su ciclo de vida, minimizando las amenazas a la vez que se cumplen con los requisitos de accesibilidad, disponibilidad, integridad, confidencialidad y trazabilidad. La correlación de toda la información disponible dentro de la red, complementada con la presente en fuentes abiertas, permite una temprana detección de incidentes que posibilitan minimizar los tiempos de respuesta ante los mismos y la gestión eficiente de los recursos.

CONCLUSIONES DE LA ENTIDAD

La seguridad se ha convertido en uno de los pilares de las tecnologías de la información, por lo que es necesario contar con las herramientas adecuadas para obtener la información de la red, sistemas y puestos de usuario, que permitan tomar las medidas necesarias para la protección del dato, desde su generación y durante todo su ciclo de vida, gestionando adecuadamente los accesos, y garantizando la accesibilidad, disponibilidad, confidencialidad, integridad y trazabilidad de los mismos.

Los proyectos abordados por el Ministerio de Justicia durante los últimos años, han permitido tener una protección adecuada, con unas medidas de seguridad efectivas que a la vez permiten proporcionar al usuario todas las funcionalidades y accesos necesarios para desarrollar su actividad profesional.

Sin embargo, no se puede afirmar que el proyecto finalice aquí. Para que estas medidas sean efectivas en el tiempo, es necesario seguir optimizando día a día los sistemas de seguridad, así como implantar nuevas funcionalidades y continuar con la integración entre las soluciones en funcionamiento. El mundo de la ciberseguridad proporciona cada vez más posibilidades, de manera que el ministerio cuenta con una estrategia de mejora continua, desarrollando nuevos proyectos que ampliarán el control y la seguridad de los datos, destacando el fomento del uso de las soluciones ofrecidas por el Centro Criptológico Nacional para coordinación y gestión de los ciberataques.