CONVOCATORIA DE PREMIOS @asLAN
A PROYECTOS EN LA ADMINISTRACIÓN PÚBLICA

TÍTULO DEL PROYECTO: EL INTA DOTA A SU RED DE INTELIGENCIA ARTIFICIAL Y APRENDIZAJE AUTOMÁTICO PARA UNA PROTECCIÓN INTEGRAL

Implantado en:

ANTECEDENTES/PROBLEMÁTICA

El Instituto de Técnica Aeroespacial (INTA), Organismo Público de Investigación (OPI) dependiente del Ministerio de Defensa, ha protegido su red global con la arquitectura Security Fabric de Fortinet.

El Instituto de Técnica Aeroespacial (INTA) cuenta con una red corporativa distribuida con 15 centros por toda España (campus tecnológicos, centros de ensayos y estaciones espaciales) y gestionada por su equipo de TI desde sus oficinas centrales en el Campus de Torrejón de Ardoz en Madrid. En los últimos años el crecimiento de la necesidad de accesos a su red a través de distintos entornos, tanto de organismos públicos nacionales e internacionales (Ministerio de Defensa, RedIris, NASA, Airbus-Eads, ESA, Galileo-GSC, Telespazzio...), o desde sector privado, así como desde diferentes endpoints (portátiles, smartphones, etc.) y la multiplicación de los vectores de ataque habían generado un problema de rendimiento y estabilidad en la seguridad de la red corporativa. Ésta se había visto ralentizada por la necesidad de mantener un alto nivel de seguridad de la misma al tiempo de mantener una flexibilidad que permitiera aumentar sus funcionalidades para responder a las necesidades de los diferentes clientes y usuarios de todo el portfolio de servicios.

RETOS - OBJETIVOS PERSEGUIDOS

En referencia a esta situación de partida, **Nur Pulad, Major Accounts Manager en Fortinet España y Portugal**, ha comentado que *"ante esta problemática, se requería una solución de protección integrada y unificada que le permitiera cubrir todos los vectores del ataque, teniendo en cuenta una premisa importante: mantener un alto rendimiento de la red con la mínima carga de trabajo para su equipo de TI. La propuesta de Fortinet fue Security Fabric, una arquitectura de seguridad de extremo a extremo, colaborativa y adaptativa diseñada para ofrecer seguridad distribuida ofreciendo protección frente a amenazas, desde IoT a dispositivos remotos, a través de la infraestructura central y dentro de la nube".*

FASES DEL PROYECTO – RECURSOS EMPLEADOS

El proyecto de implantación comenzó en abril 2018 y finalizó en diciembre de 2018.

Previamente al proyecto de implantación, Fortinet, en colaboración con Tsyvalue, realizó un exhaustivo estudio de las necesidades planteadas por el INTA.

Actualmente, Fortinet proporciona formación y certificación en sus soluciones a los responsables de TI del INTA.

NUEVOS SERVICIOS, MEJORAS EN EFICIENCIA Y REDUCCIONES DE COSTE

El extenso proyecto implementado por Fortinet en el INTA ha contemplado el despliegue de las siguientes soluciones:

Despliegue de **firewalls de nueva generación FortiGate** en alta disponibilidad que permiten al INTA abordar nuevas funcionalidades, como descifrado de tráfico y análisis de tráfico cifrado. Los FortiGate ofrecen protección a la información almacenada en su *datacenter*, así como al tráfico externo procedente de otras sedes del Instituto o de Internet.

La alta capacidad de los nuevos firewalls desplegados permite inspeccionar el flujo de tráfico interno con una latencia mínima. Asimismo, permiten una virtualización del propio equipo, gracias a la capacidad de *virtual domain*, para una gestión independiente de cada cliente o entorno del INTA. De esta manera, el Instituto puede conectar de forma independiente el core de su red de acceso y el core de data center con interfaces de 100GB y 40GB respectivamente.

INTA cuenta con una solución de autenticación centralizada, ***Aruba ClearPass PolicyManager,*** para el entorno cableado e inalámbrico de todas las sedes, gracias a la integración con la solución desplegada, los FortiGate han permitido reducir la complejidad de gestión de la red proporcionando a los equipos de TI de INTA una visibilidad automatizada de las aplicaciones, los usuarios y la red. En palabras de **Ricardo Luis Cañavate, especialista en seguridad y responsable de la definición del proyecto en Tsyvalue,** partner responsable de la implantación del proyecto, "*esta integración bidireccional proporciona a la red de acceso la capacidad de anticiparse frente a amenazas, automatizar la desconexión de equipos, dispositivos y usuarios maximizando la protección de red*".

El proyecto de seguridad también ha contemplado el despliegue de la solución para la protección y análisis de las aplicaciones web del INTA con **FortiWeb**. Las aplicaciones web son el punto de entrada más vulnerable, por lo que era necesario securizar esta potencial brecha de seguridad.

Por otro lado, la extensión del teletrabajo hacía necesario proporcionar acceso seguro a los profesionales del Instituto. A su vez esta modalidad de trabajo traía consigo dos problemas de seguridad: se desconocía el tipo de dispositivo desde el que el trabajador se conectaba (si estaba infectado, actualizado, etc.) y el acceso era directo al CPD, con el riesgo que ello conlleva en cuanto a privacidad de los datos almacenados.

Para ofrecer a sus trabajadores un entorno de teletrabajo seguro a la vez que proteger los activos de la red, se desplegó la solución **FortiMail**. Al respecto de esta solución, **Jesús Garrido, CIO y Director Departamento de Tecnologías de la Información y las Comunicaciones del INTA** ha comentado que *"entre otras funcionalidades, FortiMail nos permite ofrecer a nuestros empleados correo electrónico seguro frente a los grandes volúmenes de spam, phishing de ingeniería social y compromiso de correo electrónico empresarial, aceleración de variantes de ransomware y otros tipos de malware o ataques dirigidos. Al mismo tiempo, FortiMail protege nuestros datos confidenciales, reduciendo el riesgo de pérdida inadvertida y/o incumplimiento de normativas como GDPR o PCI".* Esta solución de protección del correo electrónico se integra y correlaciona con **FortiClient**, la solución para la protección del endpoint y con **FortiToken Mobile**.

Gracias a FortiClient, se facilita la labor del administrador de sistemas que puede establecer las normas de acceso dependiente de cómo accede el usuario a la red. De esta manera, el usuario está más protegido a la vez que hay un mayor control sobre los activos de la red. Por su parte, FortiToken Mobile garantiza el acceso seguro mediante un sistema de autenticación de doble factor, de manera instantánea gracias a las notificaciones push y la gestión desde **FortiAuthenticator**, integrada con Aruba, para el entorno cableado e inalámbrico. La estructura de seguridad de Fortinet ofrece visibilidad en tiempo real en todos los dispositivos y aplicaciones.

La arquitectura integrada Security Fabric se completa con **FortiSandbox**, una solución que proporciona un entorno de análisis de posibles amenazas desconocidas de todos los ejecutables de email, web, etc. Gracias a este entorno de análisis, nativo y automático, cualquier archivo sospechoso es analizado en el Sandbox y si resulta ser malicioso, informa automáticamente al resto de soluciones distribuidas en las distintas capas de red. Los responsables de TI de INTA pueden establecer sus propias reglas para el análisis de los archivos antes de su ejecución, liberándose de esta ardua tarea y evitando la infección de la red.

El equipo de TI dispone de una total visibilidad de todos los eventos que se producen en la red gracias a distintas soluciones: **FortiManager** para una gestión centralizaday **FortiAnalyzer** para la generación de informes de lo que ocurre en la red y **FortiSIEM** para el análisis de eventos de seguridad de cualquier plataforma y auditorías de seguridad, de SOC y NOC. Uno de los valores diferenciales de la propuesta de Fortinet que más valoró el INTA fueron el aprendizaje automático proporcionado a través FortiSIEM. Concretamente, **FortiSIEM** ofrece análisis de comportamiento del usuario y entidad (UEBA, según sus siglas inglés), aprovechando el aprendizaje automático para mejorar su detección avanzada con nuevas características de UEBA en FortiSIEM versión 5.0 gracias a su capacidad para aprender los patrones en el comportamiento típico del usuario como ubicación, hora del día, dispositivos utilizados y los servidores específicos que fueron accedidos. FortiSIEM notifica automáticamente a los equipos de operaciones de seguridad para su investigación cualquier actividad anómala que se produce en la red, como inicios de sesión simultáneos desde ubicaciones separadas, usuarios que acceden a datos corporativos en medio de la noche e inicios de sesión excesivos a servidores raramente utilizados.

Por último, Fortinet proporciona, a través de su **NSE Xperts Academy**, formación tanto a **Tsyvalue,** partner responsable del proyecto, como a los profesionales de TI del INTA, la formación y la certificación oficial en tecnologías Fortinet para que estos puedan sacar el máximo rendimiento a su nueva arquitectura de red. Asimismo, los especialistas de Fortinet realizan un seguimiento pormenorizado del despliegue adaptando las funcionalidades de las soluciones a las necesidades del cliente.

CONCLUSIONES DE LA ENTIDAD

El despliegue del tejido integral Fortinet Security Fabric ha proporcionado al Instituto de Técnica Aeroespacial (INTA) la protección y visibilidad de cada segmento de red y dispositivo, ya sea virtual, en la nube o se encuentre alojado en sus centros de datos. Asimismo, la solución de seguridad permite al INTA cumplir con las diferentes políticas de seguridad aplicadas desde los diferentes ámbitos como el estatal (ENS, GDRP, CCN STIC …), del propio Ministerio de defensa o corporativas, gestionar sus respuestas de manera sincronizada ante amenazas procedentes de cualquier elemento de la red y monitorizar y gestionar todas las soluciones desplegadas desde una única consola, lo que redunda en menores costes de gestión y personal.