PLATAFORMA DE SEGURIDAD FLEXIBLE Y VIRTUALIZADA EN LA COMUNIDAD DE MADRID.

Implantado en:
Agencia de Informática y Comunicaciones de la Comunidad de Madrid

Comunidad de Madrid

ANTECEDENTES/PROBLEMÁTICA

ICM es la Agencia de Informática y Comunicaciones de la Comunidad de Madrid. Presta sus servicios a todas las consejerías de la Comunidad de Madrid ofreciendo de manera centralizada, todos los servicios IT necesarios para su trabajo diario. La centralización de servicios, la contratación centralizada y la externalización selectiva de actividades de bajo valor añadido, permiten a ICM aprovecharse de las economías de escala que su volumen de actividad genera y prestar sus servicios con una alta eficiencia.

El modelo de prestación de servicios IT en modo "Cloud" es seguido de cerca por ICM, en particular por su flexiblidad, bajos tiempos de provisión de nuevos servicios, bajos costes marginales y alta disponibilidad. Persiguiendo estos objetivos, ICM emprendió en 2009 un ambicioso programa de evolución tecnológica con la centralización y virtualización de sus servidores en dos CPDs redundantes.

El siguiente paso consistió en migrar y adaptar la infraestructura de seguridad implantada hasta el momento a una plataforma que permitiera obtener los beneficios citados del cloud, facilitando la provisión de nuevos servicios de manera más ágil, con menos costes de mantenimiento, al mismo tiempo que se preservaba mejoraba la seguridad e integridad de los servicios.

OBJETIVOS PERSEGUIDOS

Los objetivos del proyecto fueron los siguientes:

- **Reducción de costes de operación,** gracias a la renovación tecnológica, la simplificación de reglas de seguridad y la virtualización de los cortafuegos.

- **Simplificación de la arquitectura de seguridad,** reduciendo el número de cortafuegos físicos y posibilitando la creación inmediata de cortafuegos "ad hoc", en función de las necesidades del negocio.

- **Administración delegada,** permitiendo que determinados niveles de la operación queden delegados en terceros gracias a una reorganización de la arquitectura de seguridad, que pasa de proteger "capas" de una arquitectura de sistemas tradicional, a proteger "servicios" autocontenidos, denominados dominios seguros. En estos dominios las medidas de seguridad son independientes del resto de servicios y son un elemento más de su propia definición.

- **Incremento de la seguridad y disminución del tiempo de reacción ante amenazas**, gracias a una clara distinción entre accesos y servicios, así como a la centralización de los logs de seguridad y de las alertas.

FASES DEL PROYECTO – RECURSOS EMPLEADOS

- **Fase de análisis y de reingeniería del modelo de provisión:**
  En esta fase se indentificaron los servicios IT prestados y se agruparon en "dominios" de servicio por una serie de nuevos criterios: criticidad, similitud técnica y criterios de negocio.

  También se procedió a redefinir los roles de los usuarios, eliminando la distinción entre usuarios internos (que acceden a los servicios a través de la red corporativa) y externos (a través de internet), y proteger a los servicios IT con una misma plataforma homogénea.

- **Fase de selección de proveedores:**
  Se ofreció a distintos proveedores la posibilidad de acudir a esta licitación con sus productos mediante una prueba piloto previa. Se utilizó la prueba piloto para perfilar la definición, alcance del proyecto y se procedió a su licitación pública y adjudicación.

- **Fase de implantación y pruebas de carga:**
  Constituyó la fase más crítica al substituir equipos centrales críticos. Se procedió a la instalación del nuevo equipamiento y a la posterior migración paulatina de los servicios, comprobando en cada etapa que la nueva plataforma no presentaba problemas de rendimiento y que los mecanismos de alta disponibilidad funcionaban correctamente.

MEJORAS EN EFICIENCIA Y REDUCCIONES DE COSTE

Como consecuencia del proyecto, ICM pudo reducir sustancialmente los costes de operación de los cortafuegos críticos de sus centros de datos al no depender de varios fabricantes, unificar los contratos de mantenimiento y reducir las horas hombre necesarias para administrar esta vez, una plataforma homogénea de equipos de seguridad.

Por otra parte, este nuevo proyecto permite desplegar nuevos servicios de manera muy rápida. Por ejemplo, fue posible definir y poner en marcha nuevos dominios de servicio lógicos y delegar su administración a empresas subcontratistas para la instalación de nuevos ERP sectoriales, en cuestión de

una semana. Con el anterior modelo, el tiempo de provisión no hubiera sido inferior a 6 meses y el modelo de operación mixto con terceros hubiera sido imposible de implementar.

CONCLUSIONES DE LA ENTIDAD

A raíz de este proyecto ICM ha dado un paso decidido hacia el modelo de servicio "Cloud":

- Desacoplando los servicios de red y seguridad de la infraestructura física que los soporta, gracias a la virtualización de firewalls.
- Reduciendo los tiempos de provisión de nuevos servicios y dando un paso hacia su "automatización"
- Simplificando la gestión y operación de la plataforma de seguridad.
- Reduciendo costes de operación.
- Aumentando la seguridad de los sistemas y reduciendo los tiempos de reacción antes alertas.