Organización
Alfa Kommun & Landsting AB

País
Suecia

Solución
Panda Adaptive Defense 360 + Advanced Reporting Tool

Licencias
250

"Hasta que no sufres un ataque no te das cuenta de su valor. ¡Panda Adaptive Defense hace su trabajo a la perfección!"

Kasper Lejon.

IT Director
Alfa Kommun & Landsting AB

Situación

Kasper Lejon es ingeniero de sistemas y responsable de la seguridad informática de la empresa Alfa Kommun & Landsting AB.

A finales del verano de 2016, Kasper recibió una llamada de Victor Waenerlund, comercial de Panda Security. Dicha llamada no pudo ser más oportuna, puesto que en ese momento la empresa se encontraba inmersa en la búsqueda de una solución de seguridad contra el ransomware, tras haber sufrido varios ataques de ese tipo durante los últimos seis meses.

Hasta entonces, la empresa resolvía ese tipo de situaciones mediante la funcionalidad de Copias Instantáneas de Windows, así como un proceso asociado que activaban cada vez que surgía un problema de ese tipo. Esta estrategia le daba a Alfa un nivel de preparación adecuado contra estos ataques, lo que suponía un ahorro de dinero, pero resultaba insostenible a largo plazo.

La creación de Copias Instantáneas llevaba mucho tiempo, pese a que tanto Kasper como sus compañeros eran ya expertos en el uso de dicha tecnología y sabían en qué directorios mirar. Este conocimiento era fruto del tiempo dedicado a explorar el árbol organizativo de la empresa -una tarea que inicialmente suponía toda una mañana de trabajo de un grupo de ingenieros, y que se redujo posteriormente a varias horas de trabajo de un único ingeniero una vez el proceso quedó establecido. Sin embargo, dicha tarea seguía siendo demasiado larga teniendo en cuenta además la relativa frecuencia de los ataques. Por otra parte, los usuarios de la red también se veían afectados ya que no podían utilizar sus equipos durante la realización de las tareas de 'descontaminación' y restauración.

El punto de inflexión y la decisión de dejar de utilizar la solución anterior vino motivada por un cliente en concreto, un periódico, que debía recibir una serie de archivos cifrados. ¿Qué pasaría si dichos archivos fuesen robados y se revelasen las fuentes? Alfa se dio cuenta de que carecían de una protección que pudiese ayudarles en tal situación.

Solución

Gracias a la solución Panda Adaptive Defense 360, Alfa no se ha visto afectada por ningún problema de seguridad, en contraste con la situación anterior. El servicio interviene en cuanto detecta un elemento desconocido, impidiendo su ejecución hasta que es analizado. El proceso dura un máximo de 24 horas hasta que la persona afectada puede acceder al programa deseado, aunque en la mayoría de casos ese tiempo es inferior a una hora. La alternativa, consistente en establecer distintas configuraciones en Windows, es un proceso demasiado largo. Cerrar todo el entorno para dejar abierto sólo aquello que se necesita lleva demasiado tiempo. Es una estrategia que sólo funciona en teoría y requiere de demasiada intervención en la práctica.

Panda Adaptive Defense 360 permite ahorrar tiempo y energía mediante la aplicación de una estrategia automatizada. Todo ataque recibido va seguido de su informe correspondiente. De esta forma, Kasper puede ver el perfil afectado y hacer un seguimiento hasta llegar al usuario atacado y eliminar la amenaza o vulnerabilidad de seguridad pertinente. Ahora, Alfa puede ver exactamente todo lo que sucede y cuál es su origen. En la mayoría de casos el origen de los ataques es el correo electrónico. Un usuario recibe un correo malicioso y ejecuta el malware, pero el sistema lo bloquea y el departamento de IT recibe un informe sobre el ataque neutralizado. Este método innovador de protección impide la ejecución de ataques, actuando de forma proactiva y adelantándose a los hackers.

Tal como explica Kasper: “Hasta que no sufres un ataque no te das cuenta de su valor. Ahora entiendo mejor el producto, e incluso recomiendo su uso a la gente que conozco. Por ejemplo, a un amigo cuya empresa trabaja con un entorno basado exclusivamente en Citrix. Normalmente, hasta que no sufren un ataque no suelen estar muy interesados en el producto, pero la situación cambia cuando su entorno es vulnerable y reciben un ataque. También hablé con dos empleados de una clínica médica. Para ese tipo de organización es absolutamente fundamental proteger la información confidencial de forma adecuada. Incluso para una empresa que no sea muy grande, el coste del servicio es muy pequeño en comparación con lo que puede pasar si se produce una fuga de información tras un ataque.”

Por otra parte, Alfa se está preparando para la entrada en vigor de la nueva normativa de protección de datos de carácter personal (RGPD), en 2018. Advanced Reporting Tool, un módulo adicional incluido en Adaptive Defense, permite la detección de todo tipo de ataques y el seguimiento de todas las acciones realizadas durante un intento de intrusión. Esta información es muy útil a la hora de generar informes, ya que la alternativa, consistente en no saber qué es lo que sucede en la red, puede tener consecuencias muy costosas.

Perfil de Cliente

Alfa Kommun & Landsting es una empresa que lleva desarrollando sistemas para el sector sanitario público y privado desde 1998. Alfa es líder del mercado en recetas electrónicas y sistemas de gestión de atención domiciliaria y firma digital de acuerdo a la Normativa Sueca de Asistencia Social y Sanitaria.

Evaluación

¿Cómo se comporta Panda Security como proveedor? Kasper ha tenido oportunidad de contactar con el soporte de Panda en varias ocasiones - destacando un par de ellas en las que, pese a plantear consultas complejas, la respuesta fue perfecta. Victor Waenerlund, comercial de Panda, suele contactar frecuentemente con Alfa, asegurándose de que la empresa mantiene un alto nivel de satisfacción, algo más que probable teniendo en cuenta el contacto tan cercano.

Todas las expectativas que Alfa pudiera tener sobre el servicio se han visto superadas. “Adaptive Defense hace su trabajo a la perfección. Es excelente”, concluye Kasper. La impresión general es “Muy buena. Nos sentimos protegidos y Victor cumple siempre. El servicio funciona muy bien. Creo en este producto.” Para finalizar, Kasper añade lo siguiente: “Si alguien me pregunta sobre una solución que funcione, mi respuesta es ‘Panda’”.