



2023



La Fundação CASA eleva la madurez de la ciberseguridad con una expansión más allá del endpoint

La institución vinculada a la Secretaría de Estado de Justicia y Ciudadanía incorporó los servicios Kaspersky Managed Detection and Response para aumentar la protección de forma preventiva, automática y con monitorización 24x7 en medio de un escenario cambiante con la transformación digital

Fundação CASA

Institución vinculada a la Secretaría de Estado de Justicia y Ciudadanía, la Fundação Centro de Atendimento Socioeducativo ao Adolescente (CASA) tiene como misión implementar medidas socioeducativas de acuerdo con las directrices y normas establecidas en el Estatuto del Niño y del Adolescente (ECA) y en el Sistema Nacional de Apoyo Socioeducativo (SINASE).

La Fundação CASA presta asistencia a jóvenes de entre 12 y 21 años incompletos en todo el estado de São Paulo. En 2015, la Fundação CASA/SP llegó a 149 centros socioeducativos en todo el Estado de São Paulo: 108 son de internamiento, 53 de internamiento provisional, 10 de atención inicial y 27 de semilibertad.

También es gestora del sistema socioeducativo paulista, según el Plan Decenal de Atención Socioeducativa 2014 del Estado de São Paulo. La institución promueve estudios y planifica soluciones destinadas a atender a los adolescentes infractores. En São Paulo, desde 2010, la ejecución de las medidas socioeducativas abiertas -libertad asistida y servicio comunitario - es responsabilidad de cada municipio.

Nuestra relación con Kaspersky se remonta a mucho tiempo atrás y la actualización se implementó para que estemos preparados frente a las nuevas amenazas de manera preventiva”

Julio Signorini, CIO

La pandemia del Covid-19 impuso nuevos escenarios y desafíos a las organizaciones y aceleró fuertemente la transformación digital. Con parte de los empleados trabajando remotamente y la inclusión de visitas virtuales y teleaudiencia para adolescentes que atienden medidas socioeducativas, la Fundação CASA aprovechó una asociación que ya existía desde 2016 con Kaspersky para actualizar las soluciones y aumentar su ciberseguridad.

A mediados de 2022, Fundação CASA hizo la transición de la solución Kaspersky Endpoint Security for Business Advanced a la solución Kaspersky Optimum Security que incorpora EDR, a una solución más holística: Kaspersky Optimum Security, que incluye Kaspersky EDR Optimum, con su EDR básico fácil de usar y funcionalidades robustas de EPP y Kaspersky MDR Optimum. MRD es un servicio avanzado de seguridad gestionada que proporciona inteligencia de ataque, caza de amenazas y monitorización de seguridad 24x7 para escanear, detectar y eliminar continuamente las amenazas dirigidas a su organización.

La actualización aumentó el nivel de ciberseguridad de la institución, mejorando mucho la gestión de los dispositivos y la protección de los datos institucionales, como explicó Julio Signorini, CIO de la Fundação CASA/SP. "Ahora tenemos visibilidad de micro- incidencias, recibimos feedback de posibles amenazas y sabemos cuáles son las vulnerabilidades del parque en las que tenemos que fijarnos más. Es algo que no teníamos en el pasado", afirma Signorini.

Además, al ampliar el alcance con Kaspersky, el equipo de tecnologías de la información (TI) de la Fundação CASA ha ganado más tiempo para realizar otras funciones dentro del departamento que atiende completamente a la institución, brindando service desk, contact center, DevOps, entre otros. El equipo de ciberseguridad cuenta con seis profesionales. "Hoy, gracias a MDR, somos capaces de tener una visión macro de la institución, de todo el entorno informático, y somos capaces de actuar en lo micro incluso con un equipo magro", explicó el CIO.

La interacción con el equipo de profesionales especializados de Kaspersky es constante y los informes son diarios. "Cuando hay algo que tratar, tenemos mucha agilidad para mitigar cualquier posibilidad de infección. Cuando hay un incidente, se nos comunica inmediatamente", añadió Signorini.

Un paso más allá

La Fundação CASA adoptó las soluciones de Kaspersky en 2016, cuando decidió cambiar de fabricante debido a un ataque de ransomware. Desde entonces, la institución nunca se ha enfrentado a ningún problema. Tras el éxito del caso, la entidad local, que presta asistencia a jóvenes de entre 12 y 21 años incompletos insertos en las medidas socioeducativas de privación de libertad (internamiento) y semilibertad, decidió que era el momento de confiar en soluciones más eficientes. Así, aprovechó la renovación de licencias para elevar el nivel de ciberseguridad, contratando los servicios de MDR y empezando a contar con los profesionales de Kaspersky SOC a mediados de 2022.

Inicialmente, la base estaba en 4.500 licencias de Kaspersky Endpoint Security for Business Advanced, una herramienta que incluye varios módulos de protección de endpoints, como la búsqueda y corrección de vulnerabilidades a través de la gestión de parches, el inventario de software y hardware y el cifrado. La actualización con el MDR de última generación fue un paso más allá, tener protección continua en un servicio que combina tecnologías de detección, incluidas técnicas de máquina aprendiendo.

"Enfrentábamos dificultades por el equipo reducido y el tamaño de la institución Vimos una situación favorable para actualizar a MDR y tener el servicio SOC de Kaspersky trabajando con nosotros", dijo Julio Signorini.



Soluciones adoptadas

- Kaspersky Optimum Security; Kaspersky Managed Detection and Response (Kaspersky Endpoint Detection and Response Optimum)
- Kaspersky Cybersecurity Assessment

El parque de la institución es grande. Son más de 10 mil dispositivos, como notebooks, tablets y dispositivos móviles, que son utilizados para demandas corporativas y también para medidas socio-pedagógicas en la atención. Los dispositivos también son utilizados para teleaudiencia, interacción remota con los adolescentes y para las visitas virtuales que fueron implementadas en la pandemia.

Además, la Fundação CASA gestiona informaciones de diversas categorías, como, por ejemplo, los datos del adolescente tutelado por el Estado. "Nuestro grado de seguridad tiene que ser mayor, precisamente por la criticidad de los datos", señaló el director de informática de la Fundação CASA/SP.

Otro punto que llevó a la migración fue el creciente volumen de información de la institución, que llevó a la necesidad de un seguimiento más estrecho de las aplicaciones propietarias - la Fundação CASA tiene una fábrica de software y también presta servicios a otros organismos.

"Agregamos una serie de funcionalidades para tener un nivel más amplio de ciberseguridad. Nuestra relación con Kaspersky se remonta a mucho tiempo atrás y la actualización se implementó para que estemos preparados frente a las nuevas amenazas de manera preventiva", atestiguó Julio Signorini. "Somos conscientes de la existencia de amenazas avanzadas y persistentes y muchas veces es posible detectarlas con una solución EPP, pero es muy importante tener capacidad analítica y este módulo para tener visibilidad y permitir que el ciclo de respuesta a incidentes funcione correctamente", explicó Milton Acevedo, quien dirige el área de servicios profesionales de Kaspersky.

Amenazas continuas

Hoy en día, las amenazas son persistentes y avanzadas y requieren profesionales cualificados de apoyo. No todas las organizaciones pueden contratar a este tipo de especialistas. Kaspersky Managed Detection and Response cubre este vacío, ya que ayuda en el ciclo de respuesta a incidentes, trabajando en la detección y ofreciendo recomendaciones y acciones para llevar a cabo la mitigación.

Mientras que las soluciones EPP (Endpoint Protection Platform) detectan amenazas, las soluciones EDR (Endpoint Detection and Response) dan visibilidad a elementos asociados a amenazas, por ejemplo, claves de registro, privilegios de usuario, conexiones externas, procesos de iniciación etc. "Instalamos la solución en el entorno del cliente

para recopilar información de telemetría y enviarla a nuestro SOC a través de la solución MDR. Allí nuestros expertos evalúan y dan recomendaciones 24x7. Nos apoyamos en herramientas de inteligencia artificial y en analistas cualificados dentro del centro de servicios para dar un soporte completo", explica Milton Acevedo, de Kaspersky.



9.500

funcionarios

4.500~5.000

adolescentes cumpliendo
medida socioeducativa

120

direcciones por el Estado
de São Paulo

10 mil

dispositivos

140

aplicaciones de software
publicadas

Conectividad disponible para
todos los dispositivos
en la institución

Otro aspecto esencial que está conectado con la parte de respuesta a incidentes de forma proactiva es el Kaspersky Cybersecurity Assessment, que tiene como objetivo evitar que un atacante explote una vulnerabilidad e infecte el entorno. Para ello, el equipo de Kaspersky analiza el riesgo del entorno, realizando una larga evaluación con el cliente para entender cómo se gestiona el entorno informático. Como resultado, un informe señala el nivel de riesgo de los escenarios, la cantidad de vulnerabilidades, entre otros puntos.

Implantación

Cliente desde 2016, la Fundação CASA decidió actualizarse a mediados de 2022. La implementación fue rápida, finalizando en octubre del mismo año. Luego, en noviembre, adquirió el servicio Kaspersky Cybersecurity Assessment, cuyo informe fue entregado el 27 de diciembre.

Durante los trabajos de implantación, se llevó a cabo un proceso de transferencia de conocimientos sobre el uso de la solución y se integró la solución MDR a través de Kaspersky Endpoint Detection and Response Optimum. Con esto, la institución pasó a contar con informes que señalaban incidentes en el ambiente para poder trabajar en el ciclo de respuesta.

El director de TI de la Fundação CASA/SP añadió que todo el proceso de automatización y el establecimiento de reglas de seguridad proporcionaron tranquilidad a la institución y estabilidad en el parque. Se implantaron una serie de buenas prácticas de gobernanza y seguridad de datos.

Como el entorno ya estaba adaptado a la solución de Kaspersky, la actualización se realizó sin problemas. Los equipos de la Fundação CASA y de Kaspersky colaboraron para adoptar las nuevas soluciones. "Nuestro equipo de seguridad supervisó de cerca la actualización, eso porque ha venido de ellos – del CISO, Odenilson dos Santos, y del jefe de TI, Alex Christy – partió la voluntad y la iniciativa de dar este salto", afirmó Julio Signorini.

Resultado

Con este proyecto implementado, la Fundação CASA se convierte en referencia en el mercado, elevando su nivel de madurez en ciberseguridad, al transformar un escenario de vulnerabilidades en una visión más amplia e integral a través de recursos de investigación, prevención, detección y respuesta, automatización de procesos manuales y todo esto sin altos costos ni inversiones en nuevos recursos, con total confianza.

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
IT Security for SMB: kaspersky.com/business
IT Security for Enterprise: kaspersky.com/enterprise
MSP partnership: kaspersky.com/partners

<https://latam.kaspersky.com/>

kaspersky

**BRING ON
THE FUTURE**

2023 AO KASPERSKY. ALL RIGHTS RESERVED. REGISTERED TRADEMARKS AND SERVICE MARKS ARE THE PROPERTY OF THEIR RESPECTIVE OWNERS.