



2023



Fundação CASA amplia segurança cibernética para além do endpoint

kaspersky BRING ON
THE FUTURE

Instituição vinculada à Secretaria Estadual da Justiça e Cidadania incorporou serviços MDR da Kaspersky para aumentar proteção de forma preventiva, automática e com monitoramento 24 horas por dia e 7 dias por semana, em meio à mudança de cenário com a transformação digital e ao constante crescimento da volumetria de informação

Fundação CASA

Instituição vinculada à Secretaria Estadual da Justiça e Cidadania, a Fundação Centro de Atendimento Socioeducativo ao Adolescente (CASA) tem como missão aplicar medidas socioeducativas de acordo com as diretrizes e normas previstas no Estatuto da Criança e do Adolescente (ECA) e no Sistema Nacional de Atendimento Socioeducativo (SINASE).

A Fundação CASA presta assistência a jovens de 12 a 21 anos incompletos em todo o Estado de São Paulo. Em 2015, a Fundação CASA/SP alcançou 149 centros socioeducativos em todo o Estado de São Paulo: 108 são de internação, 53 de internação provisória, 10 de atendimento inicial e 27 de semiliberdade.

A autarquia também é a gestora do sistema socioeducativo paulista, conforme o Plano Decenal de Atendimento Socioeducativo do Estado de São Paulo de 2014. A instituição promove estudos e planeja soluções direcionadas ao atendimento de adolescentes autores de ato infracional. Em São Paulo, desde 2010, a execução das medidas socioeducativas de meio aberto – liberdade assistida e prestação de serviços à comunidade – cabe a cada município.

“Nossa relação de sucesso com a Kaspersky é de longa data e o upgrade foi uma prevenção”

Julio Signorini, CIO

A pandemia da Covid-19 impôs novos cenários e desafios às organizações e acelerou fortemente a transformação digital. Com uma parte dos funcionários trabalhando de forma remota e a inclusão de visitas virtuais e teleaudiências para os adolescentes cumprindo medida socioeducativa, a Fundação CASA se aproveitou de uma parceria que já existia desde 2016 com a Kaspersky para fazer um upgrade das soluções e incrementar sua segurança cibernética.

Em meados de 2022, a Fundação CASA passou da solução Kaspersky Endpoint Security for Business Advanced para uma solução mais holística, o Kaspersky Optimum Security, que inclui o Kaspersky EDR Optimum, com EDR básico fácil de usar e funcionalidades robustas de EPP e Kaspersky MDR Optimum. O MDR é um serviço gerenciado avançado de segurança que fornece inteligência contra ataques, busca por ameaças e faz monitoramento de segurança 24x7 de forma a pesquisar, detectar e eliminar continuamente as ameaças direcionadas à sua organização.

O upgrade ampliou o nível de segurança cibernética da instituição, melhorando consideravelmente o gerenciamento de dispositivos e a proteção dos dados institucionais, conforme explicou Julio Signorini, CIO da Fundação CASA/SP. “Passamos a ter visibilidade das microincidências, receber feedbacks de possíveis ameaças e saber quais são as vulnerabilidades do parque que temos de olhar com mais afinco. É algo que não tínhamos no passado”, ressaltou Signorini.

Além disso, ao ampliar o escopo com a Kaspersky, o time de tecnologia da informação (TI) da Fundação CASA ganhou mais tempo para executar outras funções dentro do departamento que atende à instituição por completo, fornecendo service desk, contact center, DevOps, entre outros. O time de cibersegurança conta com seis profissionais. “Hoje, graças ao MDR, temos condições de ter uma visão macro da instituição, de todo ambiente computacional, e temos condições de agir no micro mesmo com um time enxuto”, explicou o CIO.

A interação com o time de profissionais especializados da Kaspersky é constante e os relatórios, diários. “Quando tem algo a ser tratado, temos muita agilidade para mitigar qualquer possibilidade de infecção. Quando há incidente, somos comunicados de imediato”, completou Signorini.

Um passo adiante

A Fundação CASA adotou as soluções da Kaspersky em 2016, quando decidiu trocar de fabricante devido a um ataque de ransomware. Desde então, nunca mais a instituição enfrentou problemas. Após o caso bem-sucedido, a autarquia, que presta assistência a jovens de 12 a 21 anos incompletos inseridos nas medidas socioeducativas de privação de liberdade (internação) e semiliberdade, decidiu que era hora de contar com soluções de maior eficiência. Assim, aproveitou a renovação das licenças para elevar o nível de segurança cibernética, contratando os serviços MDR e passando a contar com os profissionais do SOC da Kaspersky em meados de 2022.

A fundação estava inicialmente com 4.500 licenças do Advanced, ferramenta que inclui vários módulos de proteção de endpoints, tais como encontrar e corrigir vulnerabilidades. O upgrade com EDR de última geração representou um passo além, passando a contar com proteção contínua 24 horas por dia, sete dias por semana, em um serviço que combina tecnologias de detecção, inclusive com técnicas de machine learning. “Estávamos enfrentando dificuldades por conta do time reduzido e do tamanho da instituição. Vimos uma situação favorável para fazer o salto para MDR e ter o SOC da Kaspersky trabalhando conosco”, disse Julio Signorini.



Soluções adotadas

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

O parque da instituição é grande. São mais de 10 mil dispositivos, como notebooks, tablets e dispositivos móveis, que são usados para demandas corporativas e também para as medidas sócio-pedagógicas do atendimento. Os dispositivos também servem para a realização das teleaudiências, interação remota com adolescentes e para as visitas virtuais que foram implementadas durante a pandemia.

Ademais, a Fundação CASA gerencia informações de diversas categorias, como, por exemplo, o dado do adolescente que é tutoriado pelo Estado. “Nosso grau de segurança tem de ser maior, justamente pela criticidade do dado”, apontou o diretor de TI da Fundação CASA/SP.

Outro ponto que levou à migração foi o crescimento da volumetria de informação da instituição, culminando na necessidade de um acompanhamento mais de perto das aplicações proprietárias — a Fundação CASA tem fábrica de software e também presta serviço para outros órgãos.

“Agregamos uma série de funcionalidades para ter uma segurança maior e além do endpoint. Nossa relação de sucesso com a Kaspersky é de longa data e o upgrade foi uma prevenção”, atestou Julio Signorini. “Quando olhamos as ameaças, elas são avançadas e persistentes e, muitas vezes, você pode detectá-las com a solução endpoint, mas você precisa ter capacidade analítica e este módulo dá a visibilidade e permite trabalhar corretamente o ciclo de resposta a acidentes”, explicou Milton Acevedo, que administra a área de serviços profissionais na Kaspersky.

Ameaças contínuas

Atualmente, as ameaças são persistentes e avançadas e requerem profissionais qualificados no suporte. Nem todas as organizações conseguem contratar este tipo de especialista. O MDR supre esta lacuna, já que ajuda no ciclo de respostas a incidentes, trabalhando na detecção e oferecendo recomendações e ações para realizar a mitigação.

À diferença de soluções Endpoint Protection Platform (EPP), que detecta e elimina, o Endpoint Detection and Response Optimum (EDRO) dá a visibilidade dos elementos associados com ameaças, por exemplo, chaves de registro, privilégios de usuário, conexões externas, processos iniciais, etc. “Instalamos a solução no ambiente do cliente para fazer coleta das informações por telemetria e enviá-las ao nosso SOC por meio da solução MDR. Lá, nossos especialistas avaliam e dão recomendações 24x7. Contamos com ferramentas de inteligência artificial e analistas qualificados dentro do centro de serviços para dar todo suporte”, detalhou Milton Acevedo da Kaspersky.



9.500
funcionários

4.500~5.000
adolescentes cumprindo
medida socioeducativa

120
endereços espalhados pelo
Estado de São Paulo

10 mil
dispositivos

140 aplicações
de software
publicadas

Conectividade disponível
para **todos os dispositivos**
na instituição

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

www.kaspersky.com

Outro aspecto essencial e que está conectado à parte de resposta a incidente de forma proativa é o cyber assessment, que visa a evitar que um atacante possa explorar uma vulnerabilidade e, a partir disso, infectar o ambiente. Para isso, o time da Kaspersky analisa o risco do ambiente, realizando uma longa avaliação com o cliente com o objetivo de entender como o ambiente de TI é administrado. Como resultado, um relatório aponta o nível de riscos dos cenários, a quantidade de vulnerabilidades, entre outros pontos.

Implantação

Cliente desde 2016, a Fundação Casa decidiu pelo upgrade em meados de 2022. A implantação foi rápida, terminando em outubro daquele ano. Na sequência, em novembro, começou o cyber assessment, cujo relatório foi entregue em 27 de dezembro de 2022.

Durante o trabalho de implementação, houve um processo de transferência de conhecimento sobre como usar a solução e foi feita a integração da solução de MDR com EDR Optimum. Com isso, a instituição passou a contar com relatórios apontando incidentes no ambiente para conseguir trabalhar no ciclo de resposta.

O diretor de TI da Fundação CASA/SP acrescentou que todo o processo de automatização e o estabelecimento de regras de segurança proporcionaram tranquilidade à instituição e estabilidade no parque. Foi implantada uma gama de melhores práticas de governança dos dados e de segurança.

Como o ambiente já estava adaptado para solução da Kaspersky, o upgrade transcorreu de forma tranquila. Os times da Fundação CASA e da Kaspersky trabalharam juntos na adoção das novas soluções. "Nosso time de segurança acompanhou de perto o upgrade, afinal, veio deles — do CISO, Odenilson dos Santos, e do head de TI, Alex Christy — a vontade de e a iniciativa de dar este salto", contou Julio Signorini.

Resultado

Com esse projeto implementado, a Fundação CASA se torna uma referência no mercado, elevando seu nível de maturidade em cibersegurança, ao transformar um cenário de vulnerabilidades em uma visão mais ampla e abrangente através dos recursos de investigação, prevenção, detecção e resposta, automatizando processos manuais e tudo isso sem custos elevados ou investimentos em novos recursos, com total confiança.

kaspersky

**BRING ON
THE FUTURE**

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