kaspersky BRING ON THE FUTURE

EDR: o que e como

No mercado, muito se fala sobre como as ferramentas de detecção e resposta de endpoints (EDR) são a próxima grande inovação. De acordo com a Gartner[1] por exemplo, "as ferramentas de EDR oferecem um método para que profissionais técnicos de gerenciamento de risco e de segurança respondam às duas principais perguntas sobre a segurança do ambiente:

- O que aconteceu aqui?
- O que está acontecendo neste momento?"

Mas o que isso significa na prática e por que é tão importante para as organizações complementar suas plataformas de proteção de endpoint (EPP, na sigla em inglês) com ferramentas de EDR e/ou de detecção e resposta gerenciadas (MDR)?

O quê

Nos últimos anos, a tendência no setor de cibersegurança tem sido que em vez das ameaças comuns, que as EPPs podem detectar e prevenir com certa facilidade, os cibercriminosos têm focado mais em ameaças evasivas, especialmente projetadas para burlar as medidas existentes de proteção de endpoint.

Um dos motivos para isso é que está ficando cada vez mais fácil (e barato) para os cibercriminosos encontrar, combinar e testar ferramentas e métodos prontos (incluindo campanhas de "alugue um malware" com suporte 24 horas por dia, 7 dias por semana). Além disso, os ataques desse tipo têm muito mais chance de darem certo do que os cenários tradicionais.

Além disso tudo, há também o aumento do trabalho remoto que está diluindo o perímetro corporativo de muitas organizações, o que facilita o entendimento de o por quê os endpoints continuarem sendo a linha de frente na batalha contra os cibercriminosos em um futuro próximo.

Mas o que acontece quando uma EPP é confrontada por um ataque de ciberameaça evasiva? Essas ameaças são difíceis de detectar, graças à variedade de técnicas de evasão que estão sendo adotadas, particularmente o uso de ferramentas legítimas e nativas do sistema. Além disso, por ficarem indetectáveis por um longo período, elas também têm o tempo necessário para explorar e se mesclarem à infraestrutura da empresa, causando grandes prejuízos, seja por meio de vazamento de dados, ataques de ransomware ou spyware ou apagando e substituindo operações.

O resultado? O impacto financeiro médio de um vazamento de dados[2] chega a U$ 101 mil para pequenas e médias empresas e a US$ 1,09 milhão para grandes corporações. Além disso, quanto mais demorada for a resposta, maior será o impacto médio, podendo chegar a US$ 118 mil e a US$ 1,34 milhão, respectivamente, no caso de respostas que demoram mais de uma semana. Com impactos dessa magnitude, em vez de se perguntar "por que deveríamos investir em EDR?", o melhor questionamento deveria ser "por que ainda não investimos nisso?

Como

O que uma ferramenta de EDR fará por você se (e quando) você investir nela? De forma simples, sempre que você receber um alerta, a ferramenta de EDR ajudará a entender de onde a ameaça veio, como ela se desenvolveu, qual é a causa dela e se ela chegou a outros hosts, ou seja, qual é a escala dela.

---

[1] Gartner — Solution Comparison for Endpoint Detection and Response Technologies and Solutions (Comparação entre soluções e tecnologias de detecção e resposta de endpoints) — Janeiro de 2020

[2] Kaspersky - IT Security Economics 2020 (A economia da segurança de TI 2020)

Se você deseja fortalecer suas defesas internas ou combater as ameaças mais recentes com orientação externa especializada, a Kaspersky pode ajudar. Nosso Kaspersky Optimum Security habilitado para nuvem permite que você atualize a proteção contra ameaças novas, desconhecidas e evasivas por meio de detecção e resposta eficazes de ameaças e monitoramento de segurança 24 horas por dia, 7 dias por semana, sem custos ou complexidade proibitivos.

Ela também guiará você por um processo simples para lidar com incidentes, que inclui etapas como identificação, contenção, erradicação, recuperação e análise de lições aprendidas para ajudar você a se preparar para ataques futuros. Por exemplo:

- **Identificação.** O que a ferramenta de EDR encontrou? Trata-se de uma ameaça comum ou séria? Existe alguma resposta necessária com base no contexto e nos detalhes sobre a ameaça e o incidente que ela criou?
- **Contenção.** O que precisa ser feito a respeito da ameaça, como isolar o host, prevenir a execução ou colocar arquivos suspeitos em quarentena?
- **Erradicação.** Usar um verificador de indicação de comprometimento (IoC, na sigla em inglês) para encontrar e excluir arquivos relacionados, juntamente com qualquer outro processo necessário para erradicar a ameaça.
- **Recuperação**. Retornar a rede ao seu funcionamento normal. Por exemplo, se um host infectado foi isolado para prevenir o espalhamento da infecção, ele poderá ser retirado do isolamento.
- **Análise de lições aprendidas.** Assim como integrar os dados de IoC às ferramentas de segurança existentes, analisar o acesso e os controles da Web, bloquear o acesso a endereços IP ou contas de e-mail específicas ou introduzir treinamento de conscientização de segurança para ajudar os funcionários a entender melhor e identificar ameaças de segurança modernas.

Resumindo: esteja você usando uma ferramenta interna de EDR e/ou MDR, a solução deve trabalhar em conjunto com a EPP para bloquear automaticamente grandes volumes de ameaças quando ocorrerem incidentes, além de permitir que você os investigue com mais eficiência. Isso significa obter mais insights sobre o que está acontecendo em segundo plano para ter um entendimento melhor das ameaças que estão sendo identificadas. Além disso, torna sua empresa capaz de responder de maneira rápida e fácil a esses ataques, bem como procurar outros dispositivos que também possam ter sido comprometidos, fortalecendo a sua postura de segurança, especialmente em relação a ameaças novas, desconhecidas e evasivas.

Se você deseja fortalecer suas defesas internas ou combater as ameaças mais recentes com orientação externa especializada, a Kaspersky pode ajudar. Com o Kaspersky Optimum Security habilitado para nuvem, você pode atualizar a proteção contra ameaças novas, desconhecidas e evasivas por meio de detecção e resposta eficazes de ameaças e monitoramento de segurança 24 horas por dia, 7 dias por semana, sem custos ou complexidade limitantes.

Saiba mais em go.kaspersky.com/pt_br_optimum

Saiba mais sobre go.kaspersky.com/optimum

Kaspersky Optimum Security

Notícias sobre ameaças cibernéticas: www.securelist.com
Notícias de segurança de TI: business.kaspersky.com
Segurança de TI para pequenas e médias empresas: kaspersky.com/business
Segurança de TI para empresas: kaspersky.com/enterprise
Portal de inteligência de ameaças: opentip.kaspersky.com
Ferramenta de portfólio interativo: kaspersky.com/int_portfolio

www.kaspersky.com.br

Estamos comprovados. Somos independentes.
Nós somostransparente. Estamos empenhados em construir um ambiente mais seguro mundo, onde a tecnologia melhora nossas vidas. Qualé por isso que o protegemos, para que todos em todos os lugares tenham oportunidades infinitas que ele traz. Traga a segurança cibernética para um amanhã mais seguro.

Saiba mais em kaspersky.com/transparency

Proven.
Transparent.
Independent.