FIREEYE™

FICHA TÉCNICA

Avaliação de Defesa contra Ransomware

VANTAGENS

- Identifique ativos com alto risco de serem afetados por ransomware
- Identifique fraquezas de segurança visadas por ransomware
- Identifique controles de acesso fracos no compartilhamento de arquivos
- Reconheça deficiências operacionais na gestão de tarefas de ransomware
- Receba recomendações e orientações altamente práticas para mitigar ataques de ransomware

Por que contar com a FireEye Mandiant?
A FireEye Mandiant está na linha de frente da inteligência em segurança cibernética e ameaças cibernéticas desde 2004. Nossos analistas estão na linha de frente dos incidentes mais complexos do mundo. Nós temos uma profunda compreensão sobre os agentes de ameaças e suas táticas, técnicas e procedimentos (*tactics, techniques and procedures*, TTPs) utilizando nossas fontes de inteligência combinadas de adversários, máquina e vítimas.

A Avaliação de Defesa Contra Ransomware foi desenvolvida com base em nossa vasta experiência de resposta e remediação desses incidentes bem como na coleta de informações sobre ameaças em ransomware emergentes e em evolução.

Visão geral
A Avaliação de Defesa Contra Ransomware da FireEye Mandiant avalia a eficácia da capacidade de uma empresa em prevenir, detectar, conter e remediar um ataque de ransomware. Os especialistas da Mandiant avaliam elementos técnicos e não-técnicos do seu programa de segurança para determinar como sua equipe responderá a um ataque de ransomware.

Os especialistas da Mandiant avaliam o impacto técnico que um ataque de ransomware pode ter sobre uma rede interna, descobrem quais dados podem ser colocados em risco ou perdidos e testam os pontos fortes e fracos da capacidade dos seus controles de segurança em detectar e responder a ataques de ransomware.

Metodologia
A Avaliação de Defesa Contra Ransomware inclui análise de documentação, análise de configuração de logs, workshops de aprofundamento e simulações de comportamento de ataques de ransomware do mundo real.

A Avaliação de Defesa Contra Ransomware se concentra em quatro competências fundamentais de ransomware:

- **Arquitetura de segurança.** As tecnologias, controles e redes de segurança necessários para se defender de um ataque de ransomware e continuar as operações comerciais.
- **Resposta.** Os recursos de uma empresa para responder rapidamente e conter ataques de ransomware.
- **Comunicações.** Processos de comunicação internos e externos usados para entregar mensagens corporativas às principais partes interessadas (stakeholders). Inclui coordenação com seguro cibernético e assessoria jurídica.
- **Recuperação.** Os processos e a abordagem para corrigir ou se recuperar de um ataque de ransomware.

Nossas simulações de comportamento de ataque ransomware do mundo real:

- Fazem uma varredura para verificar vulnerabilidades do Windows exploradas por ransomware
- Fazem uma varredura em compartilhamentos de arquivos acessíveis que podem ser acessados por ransomware
- Simulam movimento lateral de ransomware realizando uma tentativa de explorar vulnerabilidades descobertas ou reutilizar credenciais obtidas
- Testam a segmentação entre redes para determinar se o ransomware pode se espalhar para outros ambientes como:
  - Redes de manufatura e fábrica
  - Redes de infraestrutura de backup
  - Redes de varejo
  - Outras redes seguras
- Simulam comportamento de criptografia de ransomware usando uma ferramenta de emulação de ransomware não destrutiva para reproduzir a criptografia de arquivos em massa
- Utilizam técnicas usadas por agentes de ameaças para implementar ransomware

Duração e Resultados

A Avaliação de Defesa Contra Ransomware leva normalmente uma semana. Ela pode ser realizada no local ou remotamente.

Após a contratação, a Mandiant oferece um relatório que inclui:

- Resumo executivo com os pontos fortes e áreas de melhoria
- Informações técnicas sobre o processo de teste
- Conclusões detalhadas e categorizadas por gravidade
- Resumo executivo

Para saber mais sobre a FireEye, visite: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

Sobre a FireEye, Inc.

A FireEye é a empresa líder em segurança orientada por inteligência. Atuando harmoniosamente como extensão expansível das operações de segurança dos clientes, a FireEye oferece uma plataforma única que mescla tecnologias de segurança inovadoras, inteligência de ameaças em nível governamental e a consultoria mundialmente reconhecida da Mandiant®. Com essa abordagem, a FireEye elimina a complexidade e o fardo da segurança cibernética para organizações empenhadas em se preparar, prevenir e reagir a ataques cibernéticos.

FIREEYE™