Como quebrar a cadeia de ataques de ransomware

Cinco etapas para bloquear o movimento lateral

O ransomware não se espalha violando uma única máquina ou dispositivo. Os cibercriminosos usam essa variedade de malware para criptografar o máximo possível de uma rede e garantir que as vítimas paguem o resgate.

A cada dois segundos

Até 2031, espera-se que o ransomware ataque uma empresa, consumidor ou dispositivo a cada 2 segundos.

Relatório de mercado da Cybersecurity Ventures sobre ransomware

Você confia na sua segurança de rede atual?

Se você ainda confiar em firewalls legados para segmentação, não pode impedir que o ransomware se espalhe pela sua rede e bloqueie sua infraestrutura e aplicações críticas.

A cadeia de destruição do ransomware

1. **Posição inicial**
   (Spear) Phishing ou serviços vulneráveis
2. **Movimentação lateral**
   Espalha-se pela rede para causar o máximo de impactos
3. **Filtragem**
   Localizar e roubar dados valiosos
4. **Criptografia**
   PKI para criptografia para evitar quebra de código/decodificação
5. **Nota de resgate**
   Papel de parede, e-mail, arquivo .txt de resgate etc.
6. **Impacto**
   Dados, financeiro, marca etc.

As violações são inevitáveis

Você precisa de uma solução de segurança que detecte ameaças no tráfego do data center leste-oeste e bloqueie o movimento lateral.

Quebrar a corrente

Prepare-se identificando todas as aplicações e ativos em execução em seu ambiente de TI

Previna criando regras para bloquear técnicas comuns de propagação de ransomware

Detecte recebendo alertas sobre qualquer tentativa de obter acesso a aplicações segmentadas e backups

Corrija iniciando medidas de contenção e quarentena de ameaças quando um ataque for detectado

Recupere com recursos de visualização que suportam estratégias de recuperação em fases

Em 2022, os ataques de ransomware aumentaram quase 13%, um aumento tão grande quanto nos últimos cinco anos combinados.

Verizon 2022 Data Breach Investigations Report

Se você não está preparado para se defender de ataques mais frequentes e pedidos de resgate mais caros, é hora de incorporar segmentação e visibilidade à sua estratégia de defesa.

Saiba mais

 | Suporte | Publicado em 05/23