Cinco etapas para a proteção contra ransomware

Como fortalecer suas defesas além do perímetro

SUMÁRIO

Introdução

O aumento e a disseminação do ransomware

O ransomware, que antes era simplesmente um tipo de malware incômodo usado por agentes de ameaças para restringir o acesso a arquivos e dados por meio de criptografia, se transformou em um método de ataque de proporções épicas. Embora o risco da perda permanente de dados por si só seja preocupante, os cibercriminosos e hackers de estados-nações tornaram-se sofisticados o suficiente para usar o ransomware para se infiltrar e prejudicar grandes empresas, governos estaduais e locais, infraestrutura global e organizações de saúde e muito mais. Muitos desses grupos estão até oferecendo seus serviços de RaaS (ransomware como serviço).

Prevê-se que os ataques de ransomware ocorram a cada dois segundos até 2031 e custem US$ 265 bilhões anualmente.

Cybercrime Magazine

Com a indústria de ransomware, quem perde é você

Em 2022, um ataque de ransomware forçou o 7-Eleven a fechar 175 lojas, pois não conseguiam usar suas caixas registradoras ou aceitar o pagamento. No início desse ano, um ataque de ransomware BlackCat a uma empresa alemã de petróleo afetou 233 postos de gasolina, com a Royal Dutch Shell tendo que redirecionar suas remessas para diferentes depósitos de suprimentos devido ao problema. O ataque Colonial Pipeline ocorreu em maio de 2021, interrompendo as entregas de petróleo e gás ao longo da Costa Leste dos EUA. E em 2020, o ataque de ransomware Snake paralisou totalmente as operações globais da Honda.

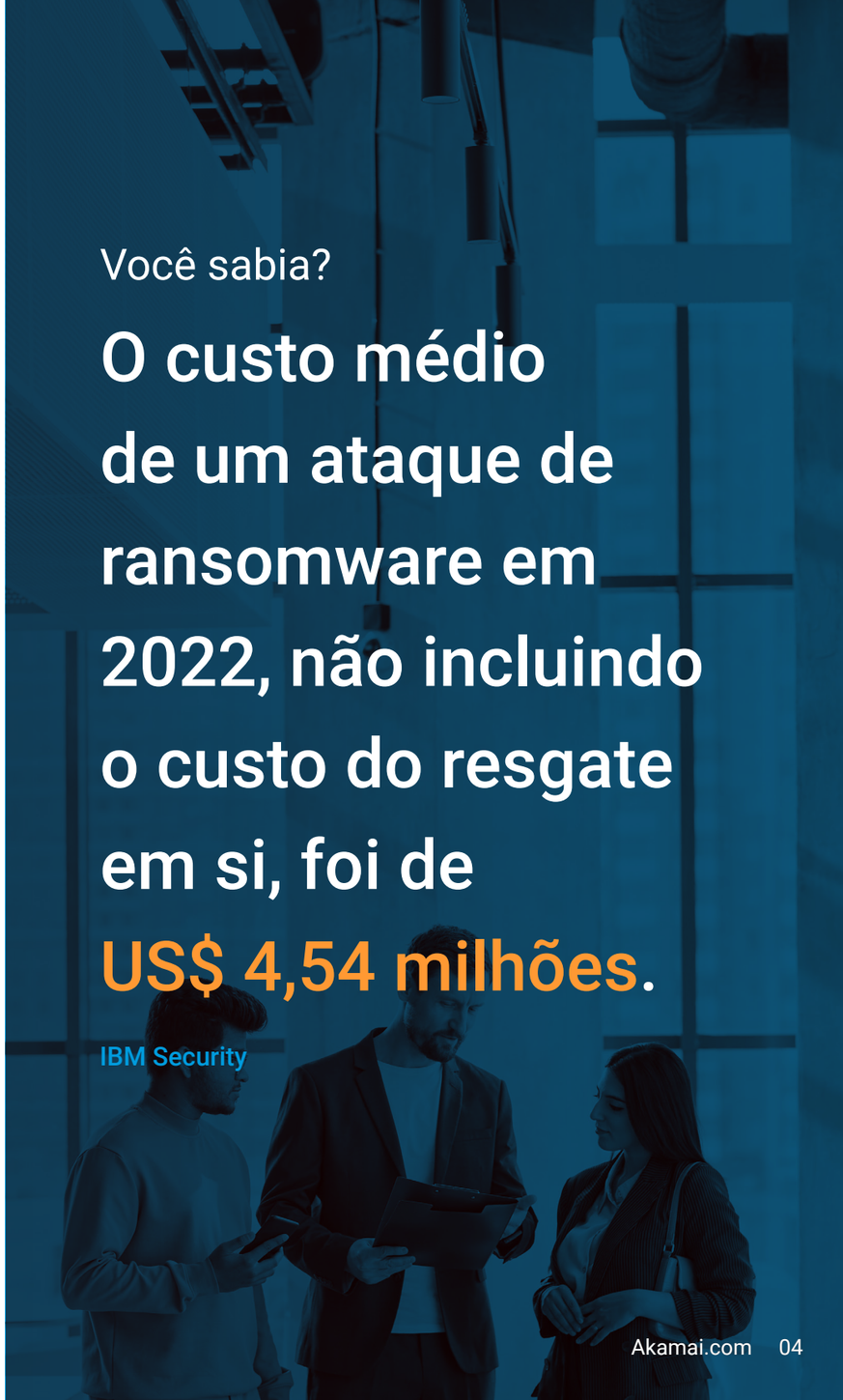
Hoje, devido a uma combinação de tecnologias desatualizadas, estratégias de defesa medianas que focam apenas em perímetros e pontos de extremidade, falta de treinamento, hábitos de segurança ineficientes e nenhuma solução garantida conhecida, organizações de todos os portes estão em risco. Os criminosos virtuais estão dedicados a criptografar o máximo possível de uma rede corporativa para extorquir um resgate que varia de milhares a milhões de dólares.

Mas há mais em jogo do que apenas as consequências mais óbvias. O resultado de um ataque de ransomware pode ser prejudicial: o tempo de inatividade pode interromper as operações de negócios, interromper a produtividade e comprometer seus dados.

Uma vez que os dados proprietários da empresa vazem ou sejam comprometidos, você provavelmente sofrerá danos à sua marca e perda da fidelidade do cliente. De acordo com uma pesquisa de 2020, 80% das violações de dados incluíam informações de identificação pessoal (PII) de clientes, a propriedade intelectual foi comprometida em 32% das violações e os dados anônimos dos clientes foram comprometidos em 24% das violações. Isso sem falar que os agentes de ameaças podem usar esses dados confidenciais contra a sua empresa ou executar outros atos insidiosos, incluindo a venda de dados confidenciais.

Com a rápida propagação da ameaça de ransomware pelas redes, a proteção do perímetro simplesmente não é suficiente.

Akamai



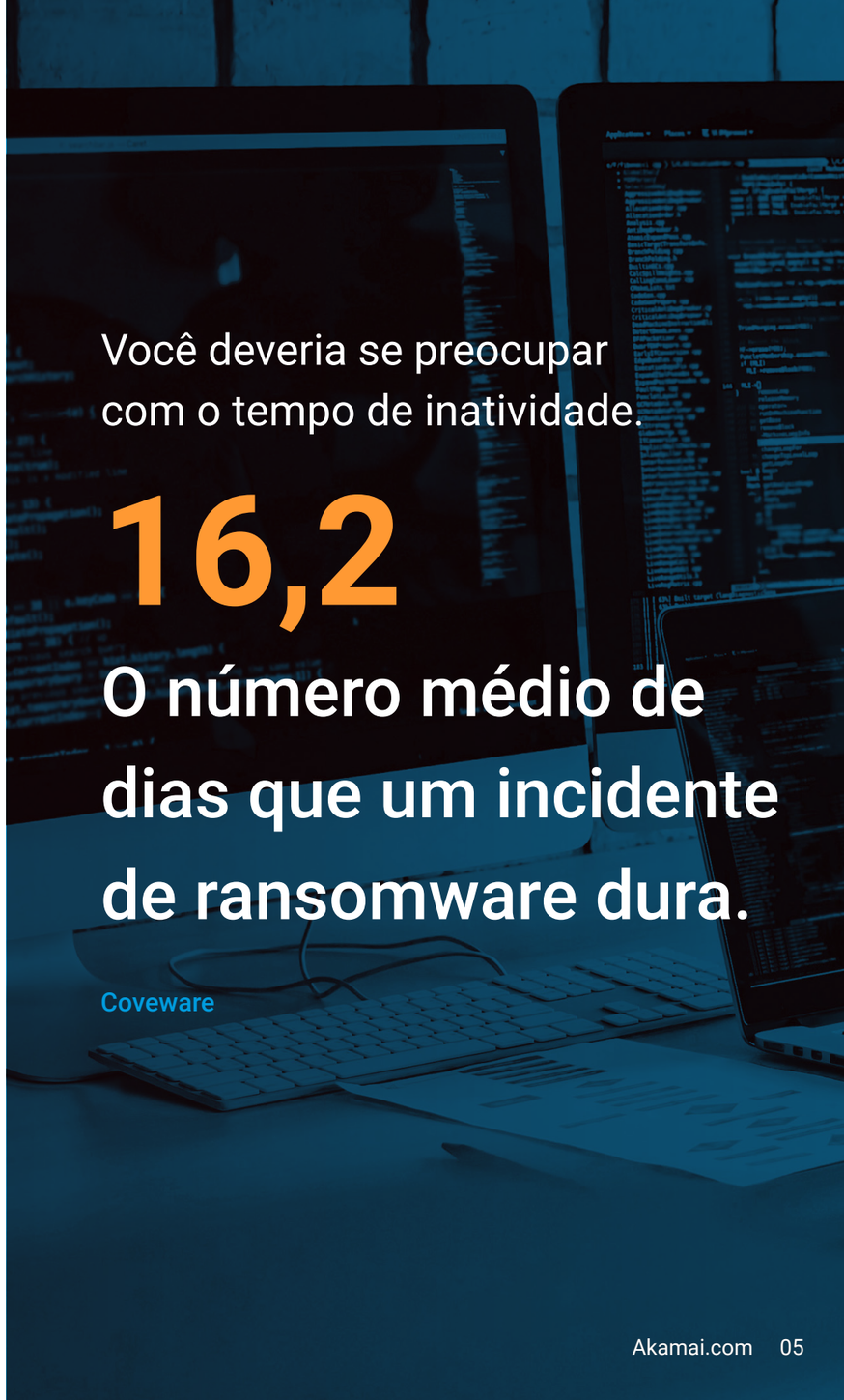
Interrompa o movimento lateral. Detenha a disseminação de ransomware.

Um ataque de ransomware começa com uma violação inicial, geralmente habilitada por um e-mail de phishing, vulnerabilidade no perímetro da rede ou ataques de força bruta que criam aberturas, enquanto desviam as defesas da intenção real do invasor.

Depois que o ataque tiver pousado em um dispositivo ou aplicação, ele continuará por meio do movimento lateral pela rede e vários pontos de extremidade para maximizar a infecção e os pontos de criptografia. Os invasores normalmente assumem o controle de um controlador de domínio, comprometem credenciais e, em seguida, encontram e criptografam o backup para impedir que o operador restaure os serviços congelados.

O movimento lateral é fundamental para o sucesso de um ataque. Se o malware não puder se espalhar além de seu ponto de chegada, ele será inútil. Portanto a prevenção do movimento lateral é essencial.

Qual é a abrangência de sua estratégia de mitigação de ameaças de ransomware?



Mitigação de riscos

Construindo uma estratégia de defesa blindada

Detectar e impedir o movimento lateral dentro de sua rede se resume a duas áreas de foco principais: primeiro, **reduza o vetor de ataque** e, depois, **limite os caminhos de propagação**.

Algumas estratégias que você pode aplicar incluem limitar a quantidade de servidores que estão expostos à Internet, acompanhar o gerenciamento de patches para garantir uma superfície de ataque menor, praticar delimitação para reduzir os caminhos de propagação entre aplicações e fazer backup de seus dados para voltar a ficar online rapidamente e evitar a perda generalizada de dados, caso ocorra um ataque.

Quatro maneiras de tornar o planejamento de segurança uma prioridade

A segurança deve fazer parte da estratégia de preparação, planejamento e orçamento mais amplos da sua organização. Isso significa aumentar a conscientização entre executivos de alto escalão e membros do Conselho e permanecer vigilante quanto aos riscos potenciais e ao que é necessário para mitigá-los.

1. Inclua a segurança virtual na função que gerencia a mitigação geral de riscos da sua organização. E certifique-se de que sua equipe de liderança ofereça expertise em segurança.
2. Não se esqueça de dedicar orçamento e recursos à geração de backup e segmentação de rede.
3. Crie planos de resposta antes de um desastre ou evento adverso (como um ataque de ransomware). Ser organizado e preparado significa que você pode reagir com mais rapidez e eficiência.
4. Analise o impacto na segurança sempre que integrar, projetar ou desenvolver novos produtos e serviços. Pergunte-se: estou abrindo uma nova porta para invasores?

Lista de verificação de detecção de ransomware

O que está acontecendo na sua rede?

Se sua organização for como muitas outras, detectar ransomware pode ser um desafio. Infelizmente, isso significa que sua rede está vulnerável a ataques. Sem fortes recursos de detecção, quando você receber uma carta de resgate, já será tarde demais: a maior parte da sua rede será criptografada ao mesmo tempo.

Quando se trata de detecção, você precisa descobrir o ransomware enquanto ele está se espalhando. Você precisará de:

Visibilidade robusta

Se você não souber o que está acontecendo na sua rede, não poderá detectar ransomware ou outras ameaças virtuais indesejadas.

Política de segmentação

Depois que cada comunicação for definida e contabilizada, qualquer coisa fora da norma subirá até a superfície e você será alertado.

Ferramentas de detecção de malware e sistema IDS

Elas detectarão as tentativas de propagação dos operadores de ransomware, usando regras e assinaturas predefinidas para vulnerabilidades ou explorações conhecidas ou com detecção de anomalias mais geral ou automatizada.

Ferramentas de engano

Preparar iscas, honeypots ou uma plataforma de engano distribuída que possa identificar movimento lateral não autorizado pode ser uma forma eficaz de descobrir uma violação ativa em andamento com incidentes de alta fidelidade.

Como construir uma estratégia de defesa contra ransomware

Apesar das melhores defesas de perímetro, violações são inevitáveis. É por isso que você deve ter uma estratégia de defesa em vigor que minimize a eficácia de um ataque e interrompa a propagação dele dentro da sua rede. Encontre um fornecedor que ofereça uma solução de segurança abrangente que detecte ameaças no tráfego do data center leste-oeste e bloqueie o movimento lateral.

Preparação

Encontre uma solução que permita identificar cada aplicação e ativo em execução no seu ambiente de TI. Esse nível de visibilidade granular permitirá que você mapeie rapidamente ativos, dados e backups críticos e identifique vulnerabilidades e riscos. Com uma visão completa do ambiente de rede, você poderá reagir e ativar rapidamente as regras durante uma violação.

Prevenção

Sua solução deve permitir a criação de regras para bloquear técnicas comuns de propagação de ransomware. Ao usar a segmentação definida por software, você pode criar microperímetros Zero Trust em torno de aplicações, backups, servidores de arquivos e bancos de dados críticos. Você também pode criar políticas de segmentação que restrinjam o tráfego entre usuários, aplicações e dispositivos, bloqueando, por fim, tentativas de movimentação lateral.

Detecção

Implemente uma solução que alerte você sobre qualquer tentativa de obter acesso a aplicações e backups segmentados. Essas tentativas bloqueadas de acesso são indicadores de movimento lateral. Além disso, você deve incorporar detecção baseada em reputação que alerta para a presença de domínios e processos mal-intencionados conhecidos. Ao permitir a rápida descoberta de ataques que violaram o perímetro com êxito, você pode minimizar o tempo de espera e capturar invasores antes que eles possam passar do ponto de chegada.

Correção

O início automático das medidas de contenção e quarentena de ameaças quando um ataque detectado é crítico. Aplique regras de isolamento que permitam a rápida desconexão das áreas afetadas da rede, enquanto as políticas de segmentação bloqueiam o acesso a aplicações críticas e backups do sistema.

Recuperação

Por fim, você precisa de recursos de visualização que suportem estratégias de recuperação em fases, nas quais a conectividade é gradualmente restaurada à medida que diferentes áreas da rede são validadas como "sem problemas".

Conclusão

Últimas considerações

Você confia na sua estratégia de defesa atual?

O ransomware veio para ficar. Na verdade, o ransomware afetou 66% das organizações em 2021, um aumento de 78% em relação a 2020, e esse número não parece estar caindo. Isso significa que o mundo continuará a lidar com uma frequência mais alta de ataques, alvos maiores e de maior valor e demandas de resgate mais caras, tudo com consequências terríveis para a sua empresa. Agora, mais do que nunca, você precisa de estratégias avançadas de planejamento e mitigação de riscos que vão além de uma abordagem somente de perímetro.

Interrompa o movimento lateral do ransomware em sua rede. Deixe a Akamai mostrar como fazer isso.

Acesse **akamai.com/guardicore** para obter mais informações.