DELL Technologies

Ransomware: Fortalecendo a resiliência e a segurança cibernética com a Dell Technologies

O que é um ransomware?

Ransomware é um tipo de software mal-intencionado (malware) que bloqueia o acesso a um sistema de computador até que um resgate seja pago. É um dos tipos mais disruptivos de ataques cibernéticos. 50% das organizações em todo o mundo foram atingidas por ransomware pelo menos uma vez no ano passado e o tempo médio de inatividade após um ataque de ransomware é de três semanas, levando a interrupções operacionais significativas

Ameaça crescente de ransomware

Ransomware é um tipo de software mal-intencionado (malware) que bloqueia o acesso a um sistema de computador até que um resgate seja pago. É um dos tipos mais disruptivos de ataques cibernéticos. 50% das organizações em todo o mundo foram atingidas por ransomware pelo menos uma vez no ano passado e o tempo médio de inatividade após um ataque de ransomware é de três semanas, levando a interrupções operacionais significativas.

Como funciona o ransomware

O ransomware geralmente infecta organizações quando alguém clica em um link mal-intencionado, abre um anexo infectado ou visita um site comprometido. Em seguida, ele entra nos sistemas para criptografar arquivos, tornando-os ilegíveis. Em seguida, o programa de ransomware geralmente exibe uma mensagem exigindo pagamento (frequentemente em criptomoedas) em troca de uma chave de descriptografia. Se o resgate não for pago, o invasor pode ameaçar excluir os dados ou divulgá-los publicamente. Um exemplo comum de ataque de ransomware que ocorreu em 2017 foi o ataque WannaCry que se espalhou rapidamente pelo mundo, afetando hospitais, empresas e agências governamentais e teve um enorme impacto financeiro. O impacto econômico global do vírus WannaCry ficou entre US$ 4 a US$ 8 bilhões, de acordo com o Cyber Risk Management (CyRiM) e o Lloyd's of London, com mais de 200.000 sistemas impactados em 150 países em questão de dias.

Duas das maiores corporações globais impactadas foram a FedEx, que relatou um prejuízo de US$ 300 milhões devido à interrupção de serviços e limpeza, e a Renault-Nissan, que teve que interromper temporariamente a produção em várias fábricas. Os custos ocultos de um ataque de ransomware podem ser muitos, incluindo:

- Tempo de inatividade e perda de produtividade da empresa
- Danos à reputação
- Custo de patches e recuperação do sistema
- Multas legais e regulatórias

Ao enfrentar um ataque de ransomware, as empresas devem tomar as seguintes medidas:

- Não realizar pagamentos, a menos que seja absolutamente necessário, não há garantia de que os invasores restaurarão o acesso.
- Restaurar a partir do backup, se disponível.
- Denunciar o ataque às autoridades.
- Fortalecer as defesas para evitar infecções futuras (por exemplo, mantenha o software atualizado, treine a equipe, use proteção de endpoint).

Combatendo ataques de ransomware com a Dell Technologies

A Dell Technologies equipa organizações com ferramentas abrangentes e inovadoras, desenvolvidas para ajudar a impedir riscos de ransomware antes que eles causem danos.

Segurança de endpoints aprimorada com Dell Trusted Devices

Os endpoints geralmente são os principais pontos de entrada para ataques de ransomware, tornando a segurança de endpoints uma área crítica de foco. Os Dell Trusted Devices integram recursos de segurança habilitados por hardware que protegem os sistemas sem comprometer o desempenho. Soluções como o Dell SafeBIOS e o SafeID fortalecem dispositivos de endpoint contra acesso não autorizado, enquanto o Dell SafeData criptografa dados para proteger informações confidenciais mesmo fora do firewall corporativo. Ao incorporar a segurança diretamente nos dispositivos, as empresas garantem proteção no nível do hardware, fornecendo aos invasores menos oportunidades de obter uma base de apoio.

Detecção proativa com a CrowdStrike

Os ataques de ransomware não são inevitáveis se as organizações usarem as ferramentas certas para detectar e responder a ameaças em tempo real. A CrowdStrike, oferecida como parte do portfólio de soluções da Dell, oferece uma plataforma de proteção de endpoints de última geração, com tecnologia de IA e análise comportamental. Essa tecnologia identifica e neutraliza atividades suspeitas antes que elas evoluam para um ataque. Ao se integrar perfeitamente à infraestrutura da Dell, a CrowdStrike permite que as equipes de TI mantenham visibilidade em todo o ambiente, fornecendo resposta imediata e eficaz às ameaças.

Proteção de dados abrangente com o Dell PowerProtect

As soluções Dell PowerProtect são o backbone da resiliência contra ransomware. Essas ferramentas avançadas de proteção de dados são desenvolvidas para proteger dados corporativos contra ameaças internas e externas. Recursos como backups imutáveis garantem que seus dados não possam ser alterados, excluídos ou criptografados por ransomware, fornecendo uma rede de segurança confiável mesmo diante de ataques avançados. O Dell PowerProtect Cyber Recovery Vault, por exemplo, isola os dados críticos da rede usando a tecnologia de "air gap", garantindo que permaneçam intocados mesmo diante das violações mais sofisticadas. Com detecção automatizada de anomalias e fluxos de trabalho inteligentes, as organizações obtêm a capacidade de detectar atividades mal-intencionadas logo no início e responder antes que o ransomware se espalhe.

Segurança de rede avançada e microssegmentação com o Dell PowerSwitch Networking e o SmartFabric OS

Fortalece as defesas contra ataques de dia zero, oferecendo segmentação de rede avançada, controles de acesso rígidos e análise de tráfego em tempo real em toda a sua infraestrutura.

Recuperação em escala com o Data Protection Services da Dell

A Dell entende que, embora a prevenção seja crítica, a recuperação é um aspecto igualmente importante da prontidão contra ransomware. O Data Protection Services da Dell fornece não apenas soluções automatizadas de backup e recuperação, mas também consultoria liderada por especialistas para garantir que as empresas possam se recuperar rapidamente e minimizar o tempo de inatividade. Serviços como recuperação remota de dados e resposta a incidentes garantem que as organizações tenham o suporte necessário durante os momentos de pico da crise. Essa abordagem abrangente garante que a integridade dos dados seja preservada e os tempos de recuperação sejam reduzidos, evitando interrupções operacionais.

Esses são apenas alguns exemplos do portfólio de soluções da Dell que podem ajudar com ameaças internas mal-intencionadas.

Pontos fortes através de parcerias

A abordagem colaborativa da Dell estende sua proteção além da tecnologia exclusiva da Dell. Por meio de parcerias com empresas líderes em segurança cibernética, como CrowdStrike e Secureworks, a Dell oferece um ecossistema de soluções integradas que abordam todos os possíveis vetores de ataque. Juntas, essas soluções fornecem cobertura de segurança completa, permitindo que as empresas criem defesas em várias camadas adaptadas aos seus perfis de risco exclusivos.

Por que escolher a Dell?

A Dell Technologies é mais do que um provedor de tecnologia, é um parceiro confiável na luta contra o ransomware. Ao combinar inovação, experiência e compromisso com a capacitação de empresas, a Dell equipa as organizações com as ferramentas e a confiança necessárias para enfrentar ameaças em evolução. Seja protegendo endpoints, dados críticos ou permitindo recuperação rápida, os produtos e serviços da Dell garantem continuidade operacional e tranquilidade.

Construindo um futuro resiliente

Os ataques de ransomware continuam a evoluir, mas com a Dell Technologies, as empresas podem estar um passo à frente. Ao aproveitar hardware, software e serviços avançados, as organizações podem criar uma estrutura de segurança cibernética resiliente, adaptável e confiável. Proteja seus dados e operações e prepare sua empresa para o futuro hoje com as soluções abrangentes da Dell contra ransomware.

Para garantir a resiliência da sua empresa, é essencial entender o cenário atual de ameaças e se manter informado sobre ameaças emergentes. Os especialistas em segurança cibernética da Dell Technologies monitoram constantemente novos vetores de ataque (como chamamos isso?) e trabalham para abordar proativamente possíveis vulnerabilidades em nossos produtos e serviços. Isso nos permite oferecer a você a proteção mais atualizada contra ameaças de ransomware em constante evolução.

Além de se manterem informadas, as empresas também devem iniciar uma abordagem de segurança em várias camadas. Isso significa implementar uma série de medidas de segurança, como firewalls, software antimalware, sistemas de detecção de invasão e backups de dados. Ao diversificar suas estratégias de defesa, você pode minimizar o impacto de qualquer ataque e garantir que sua empresa permaneça operacional mesmo diante de uma tentativa bem-sucedida de ataque de ransomware.

Também é importante testar e atualizar regularmente suas medidas de segurança (aplicar patches nos sistemas e atualizar políticas). Os hackers estão constantemente encontrando novas maneiras de contornar as medidas de segurança tradicionais, por isso é fundamental que as empresas fiquem à frente da concorrência, testando regularmente suas defesas e atualizando-as conforme necessário. Isso inclui a realização de avaliações regulares de vulnerabilidade, testes de violação e gerenciamento de patches.

Outro aspecto importante na proteção de sua empresa contra ransomware é instruir seus funcionários sobre as melhores práticas de segurança cibernética. Muitos ataques de ransomware são iniciados por meio de táticas de engenharia social, como e-mails de phishing ou links mal-intencionados. Ao instruir seus funcionários sobre como identificar e evitar essas ameaças, você pode reduzir significativamente a probabilidade de um ataque bem-sucedido.

Além disso, ter um plano de recuperação de desastres pode reduzir significativamente o impacto de um ataque de ransomware. Este plano deve incluir backups regulares de dados e sistemas importantes, bem como um procedimento claro para responder e se recuperar de um ataque.

Além dessas medidas proativas, também é importante ter um plano sólido de resposta a incidentes. Isso inclui funções e responsabilidades claramente definidas para lidar com um ataque de ransomware, bem como protocolos de comunicação para notificar as partes interessadas e reduzir danos.

Por fim, manter-se informado sobre as últimas tendências e desenvolvimentos em ataques de ransomware pode ajudar você a ficar um passo à frente de possíveis ameaças. Ao consultar regularmente relatórios do setor e atualizações de especialistas em segurança, você pode implementar proativamente novas medidas de segurança para proteger sua empresa.

Lembre-se de que nenhuma empresa está imune a ataques de ransomware, mas com as estratégias e ferramentas certas, você pode minimizar o risco e o impacto desses ataques. Ao adotar uma abordagem proativa em relação à segurança cibernética, você não está apenas protegendo seus negócios, mas também construindo confiança com seus clientes e partes interessadas.

Saiba como enfrentar alguns dos principais desafios atuais de segurança cibernética em **Dell.com/SecuritySolutions**

Saiba mais sobre as soluções Dell

Entre em contato com um especialista da Dell Technologies

Veja mais recursos

Participe da conversa com #HashTag

DELL Technologies