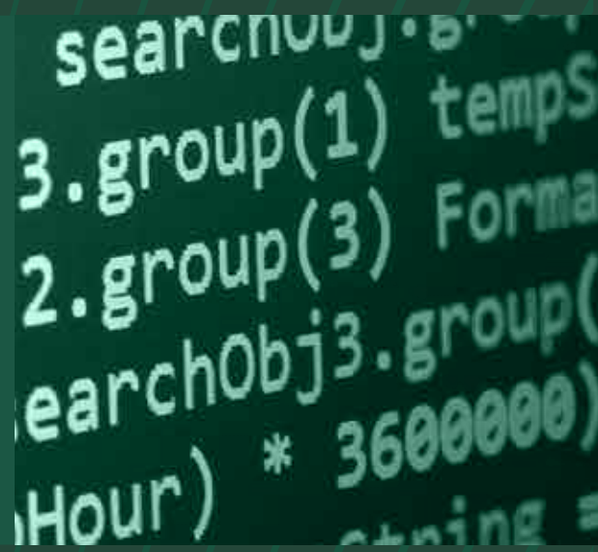
DELL Technologies

5 Recomendações para sobreviver a um ataque de ransomware



1 Mantenha um plano abrangente de resposta a incidentes

Concentre-se em minimizar o impacto de um ataque

Pratique, teste e atualize com frequência

Tenha uma equipe de resposta a incidentes pronta com antecedência

Considere o seguro cibernético como parte de sua estratégia geral de resiliência

Inclua planos para trabalhar com as autoridades competentes

2 Tenha uma estratégia de comunicação clara em vigor

Crie modelos de comunicação com antecedência

Garanta comunicações oportunas e claras dentro da organização

Prepare-se para se comunicar externamente, se for o caso

Siga as normas de notificação aplicáveis

3 Garanta proteção de dados robusta

Proteja dados essenciais em um cofre de dados isolado, imutável e com air gap

Priorize a recuperação por serviço/ infraestrutura

Pratique a capacidade de recuperação

Combine recursos como sala limpa com seu Recovery Time Objective

Garanta a integridade dos dados recuperáveis

4 Não presuma um retorno imediato à normalidade

Pagar resgate deve ser o último recurso

Garanta a conformidade com os requisitos e regulamentares legais antes de pagar

Não há garantia de que o hacker retornará seus dados, mesmo que o resgate seja pago

5 Enfatize o treinamento e a educação

Faça simulações de ataque

Monitore e teste as práticas de higiene de segurança dos funcionários

Use ferramentas como testes de phishing e treinamento de segurança de e-mail

Copyright © 2024 Dell Inc. ou suas subsidiárias. Todos os direitos reservados.

Não é mais uma questão de "se", mas "quando".

As empresas devem planejar como se um ataque fosse inevitável, apesar de suas melhores defesas. Para discutir o que fazer em caso de ataque, os especialistas da Dell, Jim Shook, Diretor global de segurança cibernética e prática de conformidade, e Steven Granat, Consultor principal de soluções de segurança cibernética e parcerias estratégicas, conversaram com Brian White, Consultor sênior de marketing de produtos do Dell Data Protection.

> "Você precisa trazer as pessoas certas, realizar um exercício e simular ações para que, quando um ataque acontecer, todos saibam imediatamente o que estão fazendo."
>
> ***Steven Granat**, Consultor principal,*
> *Soluções de segurança cibernética e parcerias estratégicas, Dell Technologies*

Mantenha um plano abrangente de resposta a incidentes

Quando ocorre um ataque, todas as principais partes interessadas — praticamente todos na organização e terceiros, como fornecedores também — devem saber o que fazer. Um plano de resposta a incidentes por escrito deve descrever uma sequência clara de ações, aconselha Shook. Um plano abrangente abordará as etapas tecnológicas, de processo e comunicação, desde a ação imediata até a recuperação. Certifique-se de manter um documento escrito em papel também, pois os modos digitais de comunicação podem não estar funcionando. "Você precisa de um plano que possa literalmente ir até a estante e pegar", diz Granat.

Tenha uma estratégia de comunicação clara

A maioria das organizações precisará se comunicar com as principais partes interessadas e, em muitos casos, precisará cumprir os requisitos regulamentares. Crie modelos diferentes para comunicações internas e externas com instruções sistemáticas sobre quem notificar e em que sequência — e quando. Planeje a inatividade de sistemas telefônicos e de e-mail.

Implemente uma estratégia de proteção de dados robusta

Um dos principais objetivos de conseguir superar um ataque de ransomware é restaurar os dados e recuperar-se da maneira mais simples possível, além de evitar o pagamento do resgate. Uma estratégia sólida de proteção de dados é uma parte fundamental para atingir esses objetivos, mas precisará incluir a tecnologia e os processos. "Use dados imutáveis e cofres cibernéticos para armazenar dados suficientes nos quais você possa confiar ou, pelo menos, como pontos de validação que permitirão recuperar sistemas", aconselha Shook. Garantir que os dados estejam protegidos é o primeiro passo. Você também deve ter as pessoas e os processos em vigor para recuperá-los. Especialistas terceirizados podem ajudar, mas eles devem ser incluídos na fase de planejamento.

Não presuma um retorno imediato à normalidade — mesmo que pague o resgate

O pagamento de um resgate, que só deve ser considerado como último recurso, não garante que o controle será restabelecido imediatamente. Lembre-se de que você está negociando com um criminoso e, mesmo que consiga as chaves de decodificação, precisará de uma estratégia para os dados recém-recuperados. Para começar, você deve testar os dados descriptografados e reconstruir todos os sistemas metodicamente. Prestar atenção redobrada aos eventos hipotéticos antes mesmo de um ataque ocorrer ajudará muito a alcançar a resiliência. "Entender os diferentes aplicativos e dependências em sua infraestrutura de tecnologia é fundamental para um retorno eficiente ao estado estável. 'Tenho uma origem de recuperação viável e um destino recuperável?', 'Tenho dados livres de comprometimento?' São considerações importantes a se fazer", diz Granat.

Na fase de recuperação, você também precisa garantir que o adversário realmente deixou seus sistemas. "Você precisa ter certeza de que o fogo foi apagado em sua casa e também descobrir o que iniciou aquele incêndio em primeiro lugar, porque sem essas duas informações críticas, você está se deixando vulnerável a ataques futuros", diz Shook.

O treinamento e a prática são essenciais

Uma parte importante da resiliência cibernética é o treinamento abrangente, que vai desde garantir que os funcionários pratiquem uma forte higiene cibernética até praticar rotineiramente o plano de recuperação. "Você precisa trazer as pessoas certas, realizar um exercício e simular ações para que, quando um ataque acontecer, todos saibam imediatamente o que estão fazendo", diz Shook.

O ransomware pode ser inevitável no atual ambiente de ameaças, mas, por meio de planejamento e execução, você pode minimizar o impacto operacional, financeiro e reputacional. O objetivo é voltar ao normal da maneira mais rápida e indolor possível.

Saiba como lidar com alguns dos principais desafios de segurança cibernética atuais em **dell.com/cybersecuritymonth**

Copyright © 2024 Dell Inc. ou suas subsidiárias. Todos os direitos reservados.

DELL Technologies