DELL Technologies

Infiltração de backups: Fortalecendo a segurança cibernética e a resiliência com a Dell Technologies

Sumário Executivo

A infiltração de backups representa uma ameaça crescente para empresas de todos os setores, explorando vulnerabilidades nos próprios sistemas projetados para proteger informações críticas. Esses ataques comprometem os sistemas de recuperação de dados, minando a confiança e colocando em risco as operações. Desde perdas financeiras significativas até tempo de inatividade prolongado e danos à reputação, as consequências podem ser graves.

A Dell Technologies oferece um conjunto completo de defesas para proteger dados confidenciais e evitar esses ataques, incluindo Dell Trusted Devices, Dell Trusted Infrastructure e amplos recursos de segurança integrados a todas as nossas soluções. Com a adição de parcerias estratégicas e serviços profissionais, a Dell ajuda as organizações a estabelecer estruturas de segurança resilientes em várias camadas para detectar, impedir e se recuperar de incidentes de infiltração de backups de forma eficiente.

Ao implementar as soluções inovadoras e o suporte especializado da Dell, as empresas estarão mais bem preparadas para proteger sua infraestrutura e manter a continuidade operacional.

Ameaça crescente de infiltração de backups

Os sistemas de backup são essenciais para a continuidade dos negócios e fundamentais na recuperação após eventos cibernéticos, como falha de hardware ou ransomware. Infelizmente, esses recursos vitais vêm sendo cada vez mais visados por criminosos cibernéticos. A infiltração de backups corrompe ou exclui os dados de backup, tornando-os inacessíveis justamente quando mais se precisa deles.

Essas ameaças em evolução exigem medidas proativas. A falha em proteger os sistemas de backup coloca em risco as operações e expõe dados confidenciais. Empresas de todos os portes, de pequenas empresas a multinacionais, são alvos potenciais, com setores como saúde, finanças e fabricação particularmente em risco.

A Dell Technologies reconhece a urgência de fortalecer ambientes de backup, oferecendo ferramentas avançadas e orientação para combater esses ataques sofisticados.

Ataques de infiltração de backups

A infiltração de backups ocorre quando criminosos cibernéticos exploram vulnerabilidades em sistemas de backup para comprometer, destruir ou criptografar dados críticos de recuperação. Esses ataques sofisticados podem coincidir ou ocorrer após outros incidentes, como a implementação de ransomware ou malware, ampliando as consequências operacionais e financeiras.

Como funcionam os ataques de backup

1. **Violação inicial:** Os invasores obtêm acesso não autorizado à rede, muitas vezes por meio de phishing, credenciais fracas ou vulnerabilidades não corrigidas.
2. **Movimento lateral:** Uma vez dentro da rede, os invasores usam ferramentas para se mover sem serem detectados, visando repositórios de backup e conjuntos de dados críticos.
3. **Comprometimento de backup:** As principais táticas incluem criptografar arquivos de backup, excluir pontos de recuperação ou corromper dados.

Técnicas comuns

- **O Roubo de credenciais** viola contas administrativas para permitir acesso total aos sistemas de backup.
- **A implementação de ransomware** criptografa dados ativos e backups, exigindo pagamento em troca da descriptografia.
- **A corrupção programada** compromete os backups de forma gradual para escapar da detecção, deixando as empresas expostas quando a recuperação é necessária.

Essas técnicas destacam a sofisticação e a gravidade dessas ameaças, exigindo ação preventiva.

O impacto nos negócios

Perdas financeiras

A infiltração de backups aumenta os custos de recuperação e o tempo de inatividade, muitas vezes dobrando ou triplicando as despesas de resposta. A recuperação de backups criptografados ou comprometidos pode exigir pagamentos a invasores, nova infraestrutura ou consultores caros.

Disrupção operacional

Sem backups viáveis, as organizações enfrentam longos tempos de recuperação que afetam os serviços, atrasam os projetos e interrompem as funções críticas.

Consequências para a reputação

Perda permanente de dados ou tempo de inatividade prolongado desgastam a confiança das partes interessadas, potencialmente prejudicando a viabilidade de longo prazo de uma empresa.

Exemplo do mundo real

Um prestador global de serviços de saúde descobriu que seus backups foram corrompidos durante um ataque de ransomware. Apesar do pagamento do resgate, três semanas de dados de pacientes foram permanentemente perdidos, atrasando cirurgias e gerando processos judiciais. Os custos totais de recuperação ultrapassaram **US$ 50 milhões.**

Estatísticas alarmantes

Estudos recentes estimam que o impacto financeiro médio causado por um sistema de backup comprometido excede **US$ 4,45 milhões**,[1] incluindo multas, tempo de inatividade e despesas de recuperação. A frequência crescente desses incidentes é particularmente alarmante, com relatórios globais mostrando um aumento anual de **39%** em ameaças relacionadas a backup.

57%
dos ataques direcionados a backups infiltram com sucesso nos repositórios de backup

Fonte: 2024: Mecanismos de indexação

Combatendo a infiltração de backups com a Dell Technologies

A Dell Technologies oferece um conjunto robusto de ferramentas e serviços para enfrentar os desafios únicos dos ataques de infiltração de backups, permitindo que as empresas evitem, detectem e recuperem de forma eficaz.

Soluções de segurança de servidor e armazenamento

As soluções de armazenamento e servidor da Dell oferecem resiliência incomparável contra esforços de direcionamento de backup. Os recursos integrados garantem que os backups permaneçam seguros e que os snapshots não sejam comprometidos.

- **Backups imutáveis/snapshots** criam pontos de restauração à prova de adulteração.
- **A Recuperação com air gap** isola dados de redes ativas para evitar corrupção.

[1] Ponemon - Cost of a Data Breach Report 2024

Fortalecendo os equipamentos Dell Data Protection

Os equipamentos Dell Data Protection são incorporados com recursos que incluem o Dell SafeBIOS para integridade do firmware e o SafeData para criptografia segura para ajudar a proteger contra ataques de backup. Além disso, essas soluções têm recursos como autenticação baseada em vários fatores (MFA), controles de acesso baseados em função (RBAC) e autenticação dupla para manter os agentes de ameaça afastados.

Detecção de ameaça avançada com a CrowdStrike

A integração entre a CrowdStrike e o Dell Data Protection se concentra em aprimorar a segurança e o monitoramento de ambientes de proteção de dados por meio de um conjunto de recursos avançados.

1. **Proteção de dados e de endpoint:** A Dell integra a segurança de endpoints da CrowdStrike e a detecção e resposta estendidas (EDR/XDR) com suas soluções de proteção de dados. Isso inclui a coleta de telemetria do PowerProtect Data Manager e do PowerProtect Data Domain da Dell, além de insights de segurança do console CrowdStrike Falcon e do software SIEM de última geração
2. **Monitorar e responder:** O serviço Managed Detection and Response (MDR) da Dell gerencia o software CrowdStrike em nome dos clientes, coletando logs e investigando qualquer indicador de comprometimento (IOC) ou detecção de anomalias. Essa integração permite que a Dell forneça monitoramento contínuo e colabore com o SOC do cliente para garantir a correção rápida e eficaz de ameaças
3. **Visibilidade em tempo real e Controle de movimentação de dados:** A plataforma CrowdStrike Falcon Data Protection oferece visibilidade em tempo real da movimentação de dados em várias fontes e canais, classificando os dados por conteúdo e contexto. Isso ajuda a prevenir o roubo de dados e garantir que as políticas de proteção de dados sejam aplicadas de forma eficaz, combinando conteúdo com análise contextual
4. **Gerenciamento unificado e implementação simplificada:** A integração permite que uma única plataforma e agente gerenciem a proteção de dados e de endpoints, reduzindo a complexidade e a sobrecarga operacional. Isso é facilitado pela abordagem leve e nativa em nuvem da plataforma CrowdStrike Falcon, permitindo implementação rápida e interrupção mínima

A integração entre CrowdStrike e Dell Data Protection aproveita recursos avançados de EDR/XDR, monitoramento em tempo real e gerenciamento abrangente de dados para aumentar a segurança geral e a resiliência dos ambientes de proteção de dados.

Recentemente, uma instituição financeira líder implementou o PowerProtect Cyber Recovery, impedindo que invasores acessassem 90% dos backups críticos durante uma violação, permitindo uma restauração perfeita sem pagamentos de resgate.

Soluções Dell PowerProtect para integridade de backup

O Dell PowerProtect oferece proteção abrangente de backup, aproveitando imutabilidade, isolamento e compactação para evitar comprometimentos do sistema de backup. Ao integrar-se com ferramentas de detecção de ransomware, o PowerProtect garante que alterações suspeitas acionem alertas para ação imediata.

A abordagem de segurança multicamadas

A proteção de dados requer estratégias de segurança coordenadas e multifacetadas. A Dell ajuda as empresas a implementar as melhores práticas do setor para criar um ambiente de backup resiliente.

Principais etapas para aprimorar a defesa

- **Adotar princípios do Zero Trust:** Valide continuamente todos os usuários, dispositivos e processos, reduzindo o risco de acesso não autorizado.
- **Criptografar todos os backups:** Garanta que os dados permaneçam ilegíveis se forem comprometidos, tanto em trânsito quanto em repouso.
- **Capacitar os funcionários:** Ensine os funcionários a reconhecer tentativas de phishing e outras táticas de engenharia social que levam a violações iniciais.
- **Testes regulares de vulnerabilidade:** Testes frequentes ajudam as organizações a identificar e corrigir áreas fracas antes que invasores as explorem.

A Dell combina essas práticas com soluções de ponta, construindo uma infraestrutura robusta e responsiva, pronta para enfrentar os desafios emergentes.

Parcerias estratégicas que aumentam a segurança

A Dell trabalha com líderes em segurança cibernética, como Microsoft, CrowdStrike e Secureworks. Cada parceria aprimora as soluções da Dell, oferecendo aos clientes recursos de proteção incomparáveis, como inteligência contra ameaças avançadas, monitoramento de endpoints e estratégias abrangentes de resposta.

Aproveitando o Dell Professional Services

Os serviços profissionais da Dell Technologies fornecem conhecimento e orientação para ajudar as empresas a enfrentar desafios complexos de segurança cibernética de forma eficaz. Da criação de planos de resposta a incidentes à implementação de arquiteturas zero trust, os especialistas da Dell garantem que os ambientes dos clientes permaneçam resilientes contra ameaças modernas, como infiltração de backups.

Desenvolva resiliência dos negócios com a Dell

Escolher a Dell Technologies posiciona as empresas para superar invasores sofisticados, mantendo a continuidade operacional. Por meio da inovação, da parceria e da experiência, a Dell garante que as organizações possam prevenir, detectar e se recuperar até mesmo dos ataques de infiltração de backups mais graves.

Dê o próximo passo

Entre em contato com a Dell Technologies hoje mesmo para proteger sua empresa. Juntos, protegeremos seus ativos críticos, protegeremos sua reputação e construiremos um futuro resiliente.

A Dell continua comprometida em promover a confiança na era digital, oferecendo às organizações as ferramentas, o conhecimento e o suporte necessários para operar com segurança e prosperar.

A resiliência de backup começa com a Dell Technologies. Aja agora para preparar suas operações para o futuro e gerar confiança em sua postura de segurança cibernética.

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

Saiba mais sobre Soluções da Dell

Entre em contato com um especialista da Dell Technologies

Veja mais recursos

Participe da conversa com #HashTag

DELL Technologies