DELL Technologies

Dia zero: Fortalecendo a resiliência e a segurança cibernética com a Dell Technologies

A ameaça crescente dos ataques de dia zero

Os ataques de dia zero se tornaram rapidamente um dos desafios mais formidáveis do cenário atual de segurança cibernética. Esses ataques exploram vulnerabilidades desconhecidas dos provedores de software e especialistas em segurança, deixando as empresas despreparadas e expostas. As organizações de todos os setores, desde a saúde até o setor financeiro, são vulneráveis a tais violações, o que muitas vezes resulta em graves consequências financeiras e operacionais.

O ritmo da transformação digital está acelerando e os ataques de dia zero tornaram-se mais frequentes e sofisticados. A necessidade de proteções robustas nunca foi tão grande. A Dell Technologies entende a natureza crítica dessa ameaça e fornece às empresas defesas inovadoras e escaláveis para combater e recuperar ataques de dia zero com eficiência.

O que são ataques de dia zero?

Um ataque de dia zero envolve a exploração de uma vulnerabilidade de segurança não divulgada em software ou hardware antes que um patch ou correção esteja disponível. Os invasores aproveitam a janela de oportunidade, muitas vezes causando uma interrupção generalizada antes que a vulnerabilidade seja descoberta e abordada.

Como os ataques de dia zero funcionam

1. **Descoberta da vulnerabilidade:** os hackers identificam falhas de codificação ou backdoors ocultos em aplicativos ou sistemas de software.
2. **Desenvolvimento de explorações:** o malware é criado para explorar a vulnerabilidade. Os invasores podem usar campanhas de phishing direcionadas ou sites infectados por malware para distribuir a exploração.
3. **Execução do ataque:** a exploração é implementada, comprometendo o sistema e potencialmente permitindo roubo de dados ou interferência operacional.

Técnicas comuns

- Os downloads automáticos (drive-by) induzem os usuários a instalar o malware sem saber.
- E-mails de phishing distribuem links ou cargas mal-intencionados para explorar vulnerabilidades.
- Os ataques sem arquivo evitam a detecção executando operações somente na memória do sistema.

Esses vetores de ataque altamente avançados tornam os ataques de dia zero particularmente perigosos, já que as ferramentas de detecção tradicionais baseadas em assinaturas muitas vezes não conseguem reconhecê-los.

O impacto sobre as empresas

Os ataques de dia zero apresentam riscos significativos devido à imprevisibilidade e ao atraso na detecção. As consequências podem ser catastróficas em várias frentes.

Perda financeira

Um ataque bem-sucedido de dia zero pode resultar em custos elevados, desde multas regulatórias até perda de receita durante o tempo de inatividade. Por exemplo, uma vulnerabilidade não identificada explorada em uma plataforma de comércio eletrônico pode desativar o processo de pagamento, afetando diretamente as vendas.

Consequências para a reputação

A percepção pública de uma empresa pode ser irreparavelmente prejudicada. Os clientes perdem a confiança quando informações confidenciais são expostas ou os serviços falham.

Disrupção operacional

As vulnerabilidades não abordadas geralmente paralisam os sistemas, causando redução da produtividade, atraso em projetos e perda de oportunidades de negócios.

Exemplo do mundo real

Um importante prestador de serviços de saúde foi vítima de um ataque de dia zero que visava o software de dispositivos médicos sem patches. O ataque interrompeu operações essenciais, expôs os dados dos pacientes e custou à organização **milhões** em taxas de recuperação, ao mesmo tempo em que desgastou a confiança do paciente.

Estatísticas alarmantes

De acordo com um estudo Ponemon de 2023, a pesquisa indica que a porcentagem de violações envolvendo ataques de dia zero é de aproximadamente 80%

Ataques de dia zero representam consistentemente mais de **70%** das vulnerabilidades exploradas

Fonte: 2024: Mandiant "M-Trends"

Combate a ataques de dia zero com a Dell Technologies

A Dell Technologies oferece soluções líderes do setor para ajudar as empresas a se protegerem ativamente contra ataques de dia zero e, ao mesmo tempo, promover uma rápida recuperação após essas violações.

Soluções de segurança de servidor e armazenamento

As soluções de segurança de servidor e armazenamento de dados da Dell fornecem camadas adicionais de proteção:

- Os servidores seguros monitoram e bloqueiam tentativas de acesso não autorizado.
- Os sistemas de backup e recuperação de dados garantem que, mesmo no pior cenário, as informações críticas permaneçam acessíveis e intactas.

Endpoints fortalecidos com Dell Trusted Devices

Os endpoints são um ponto de entrada importante para os invasores. Os Dell Trusted Devices incorporam medidas de segurança avançadas, garantindo que os endpoints permaneçam protegidos contra ameaças não descobertas.

- **O SafeBIOS** protege o firmware contra manipulação, garantindo a integridade do sistema desde o início.
- **O SafeID** protege as credenciais do usuário protegendo os processos de autenticação.
- **O SafeData** criptografa dados confidenciais em repouso e em trânsito, tornando-os inúteis em caso de interceptação ou exploração.

Detecção proativa de ameaças com a CrowdStrike

A CrowdStrike aproveita a análise avançada e a IA para monitorar a atividade de endpoints, para detectar um comportamento incomum que pode indicar explorações de dia zero. Sua detecção proativa de ameaças garante uma resposta rápida antes que as vulnerabilidades possam resultar em danos generalizados.

Por exemplo, um provedor de telecomunicações que usa a CrowdStrike conseguiu detectar anomalias no tráfego de rede logo no início, mitigando uma possível exploração de dia zero nos servidores do cliente.

Soluções Dell PowerProtect

O Dell PowerProtect oferece backups robustos e imutáveis, além de opções para recuperação isoladas. As empresas podem restaurar operações de forma rápida e eficiente após um ataque de dia zero, mantendo a continuidade dos negócios e protegendo os dados vitais dos clientes.

Por exemplo, uma grande cadeia de varejo utilizou o PowerProtect para recuperar arquivos criptografados comprometidos por um ataque de ransomware decorrente de uma vulnerabilidade de dia zero, evitando tempo de inatividade prolongado.

Segurança de rede avançada e microssegmentação com Dell PowerSwitch Networking e 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.

A importância de uma abordagem de segurança multicamadas

A verdadeira segurança requer mais de uma solução. Uma estratégia de múltiplas camadas combina tecnologia, processos e pessoas para formar uma estrutura de proteção integral.

Principais ações para fortalecer a defesa

- **Adotar os princípios de zero trust:** Verificar cada indivíduo e dispositivo que está tentando acessar a rede.
- **Implementar criptografia avançada:** Utilizar protocolos de criptografia para proteger os dados em movimento e em repouso.
- **Capacitar os funcionários:** Fornecer sessões de treinamento detalhadas para ensinar os funcionários como reconhecer tentativas de phishing e táticas de engenharia social.
- **Testar os sistemas regularmente:** Realizar testes de invasão e verificações de vulnerabilidade de forma consistente para garantir que as proteções sejam capazes de lidar com novas ameaças.

A Dell Technologies combina essas práticas com suas soluções de segurança avançadas, garantindo que as organizações estejam prontas para combater vulnerabilidades de dia zero com eficiência.

Parcerias que fortalecem a segurança cibernética

A colaboração da Dell com líderes do setor como a **Microsoft**, a **CrowdStrike** e a **SecureWorks**, oferece aos clientes acesso a ferramentas e inteligência de segurança de ponta.

- **A Microsoft** se integra perfeitamente às soluções da Dell para garantir compatibilidade em todo o sistema e mecanismos de proteção proativos
- **A CrowdStrike** oferece inteligência contra ameaças de endpoint para detectar possíveis explorações de dia zero.
- **O SecureWorks** oferece monitoramento contínuo e correção especializada para respostas a ataques em tempo real.

Aproveitando o Dell Professional Services

O Dell Professional Services oferece uma ampla gama de assistência em consultoria, implementação e recuperação para ajudar as empresas a abordar e reduzir os riscos associados a ameaças de dia zero. Desde a resposta a incidentes até o planejamento do roteiro de segurança cibernética, a Dell ajuda as organizações a obter resiliência de longo prazo.

Crie um futuro resiliente

Investir na Dell Technologies significa ter um parceiro que oferece não apenas tecnologia superior, mas também tranquilidade. Por meio de soluções de ponta, parcerias estratégicas e experiência inigualável, a Dell capacita as organizações a antecipar, detectar e se recuperar até mesmo dos ataques de dia zero mais avançados.

Entre em contato com a Dell Technologies hoje mesmo para reforçar a segurança da sua empresa, proteger sua reputação e prosperar em um cenário digital imprevisível. Confie na Dell para fortalecer seu futuro contra as ameaças do futuro.

A Dell Technologies inspira confiança, permitindo que as empresas se mantenham um passo à frente dos desafios em constante evolução dos ataques de dia zero, por meio de suas soluções e serviços de segurança desenvolvidos para proteger seus ativos mais importantes.

Saiba como lidar com alguns dos principais desafios de segurança cibernética atuais 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