DELL Technologies

Proteção contra ataques cibernéticos à cadeia de suprimentos com a Dell Technologies

Sumário Executivo

A natureza cada vez mais global e interconectada das operações comerciais expôs as organizações a crescentes ameaças de ataques cibernéticos à cadeia de suprimentos. Esses ataques sofisticados exploram vulnerabilidades no ciclo de vida do hardware, desde a fabricação até a implementação, bem como em software de terceiros, permitindo que agentes mal-intencionados comprometam sistemas inteiros por meio de aplicativos ou atualizações confiáveis. Esses incidentes não são apenas financeiramente desastrosos, mas também podem degradar reputações e interromper operações em grande escala.

As implicações dessas ameaças são profundas. Os ataques à cadeia de suprimentos geralmente passam despercebidos até que danos significativos ocorram, tornando essenciais as estratégias de defesa proativas. Com proteção avançada de endpoints, monitoramento proativo e soluções abrangentes de segurança de servidores e dados, a Dell capacita as empresas a proteger suas cadeias de suprimentos de ponta a ponta. Por meio de tecnologia, parcerias e conhecimento, as organizações podem desenvolver resiliência e se proteger das vulnerabilidades inerentes aos seus ecossistemas.

A crescente ameaça dos ataques cibernéticos à cadeia de suprimentos

Os ataques à cadeia de suprimentos aumentaram substancialmente nos últimos anos. Ao adulterar dispositivos físicos durante a produção, envio ou implementação, ou ao encontrar vulnerabilidades em provedores de software, os invasores obtêm meios de injetar componentes ou códigos mal-intencionados, corromper sistemas ou exfiltrar dados confidenciais. As vítimas variam de pequenas empresas a empresas globais, com resultados que incluem perdas financeiras graves, comprometimento da confiança do cliente e repercussões legais. A Dell Technologies reconhece esse perigo crescente e defende medidas preventivas para reduzir os impactos catastróficos desses ataques.

Compreendendo os ataques cibernéticos à cadeia de suprimentos

Como funcionam os ataques à cadeia de suprimentos de hardware

1. **Estágio de fabricação:** Os invasores introduzem componentes mal-intencionados durante a montagem do hardware, geralmente aproveitando fornecedores afetados.
2. **Fase de envio:** Os dispositivos são interceptados durante o transporte e modificados para incluir modificações prejudiciais de firmware ou hardware.
3. **Implementação e ativação:** Assim que o hardware comprometido entra na rede da organização, os invasores obtêm acesso a dados confidenciais ou realizam operações de backdoor.

Como funcionam os ataques à cadeia de suprimentos de software

1. **Violação inicial:** Um fornecedor de software de terceiros é comprometido, geralmente por meio de phishing, vulnerabilidades não corrigidas ou ameaças internas.
2. **Manipulação de código:** Agentes mal-intencionados injetam elementos prejudiciais, como malware ou backdoors, em softwares destinados à distribuição.

3. **Propagação para usuários finais:** As empresas que instalam ou atualizam softwares comprometidos fazem download inadvertidamente de componentes mal-intencionados.

Técnicas comuns — Hardware

- **Manipulação de firmware:** Incorporando código mal-intencionado que é ativado após a implementação.
- **Implantação de hardware:** Integrando componentes ocultos para monitorar ou exfiltrar dados.
- **Exploração de fornecedores confiáveis:** Utilizando fornecedores terceirizados com processos menos seguros.

Técnicas comuns — Software

- **Sequestro de componentes:** Infectando bibliotecas ou estruturas de terceiros com código mal-intencionado.
- **Comprometimento de atualizações:** Alterando atualizações oficiais de software para incluir explorações.
- **Confusão de dependência:** Explorando a dependência das organizações em pacotes inseguros.

O impacto nos negócios

Consequências financeiras

Os ataques direcionados a cadeias de suprimentos frequentemente resultam em custos envolvendo multas legais, despesas de recuperação do sistema e compensação do cliente. Um incidente de alto perfil envolvendo uma empresa global de gerenciamento de TI levou a perdas superiores a US$ 70 milhões, ilustrando o caos financeiro que essas violações podem causar.

Disrupção operacional

Sistemas corrompidos ou desativados devido à infiltração de malware geralmente resultam em longos períodos de inatividade, prejudicando a produtividade e atrasando entregas de projetos.

Consequências para a reputação

A confiança nos parceiros de software é fundamental para as empresas modernas. Uma violação da cadeia de suprimentos vinculada às ofertas de software de uma organização pode manchar reputações e desgastar a fidelidade do cliente.

Exemplos do mundo real — Hardware/software

Um fabricante global de eletrônicos descobriu componentes comprometidos em sua cadeia de suprimentos, levando a falhas generalizadas no sistema. O ataque custou mais de **US$ 45 milhões** em recuperação e honorários advocatícios, além de danos irreparáveis aos relacionamentos com fornecedores.

A violação da SolarWinds está entre os ataques mais infames à cadeia de suprimentos de software. O comprometimento do produto Orion infectou organizações em todo o mundo, incluindo agências governamentais e empresas da Fortune 500. As estimativas de danos ultrapassaram **US$ 90 milhões**, e a violação destacou as consequências de longo alcance das vulnerabilidades da cadeia de suprimentos.

Experiência da Dell Technologies no combate a ataques à cadeia de suprimentos

O amplo portfólio de soluções de segurança da Dell Technologies capacita as empresas para ficarem à frente dos riscos cibernéticos em evolução.

Dell Secure Component Verification (SCV)

O Secure Component Verification (SCV) é parte integrante da estratégia de segurança da cadeia de suprimentos da Dell Technologies, desenvolvido para garantir a autenticidade e a integridade dos componentes de hardware em várias soluções da Dell. A SCV oferece validação criptográfica dos componentes do sistema desde o momento da fabricação até a entrega e implementação. A Dell Technologies oferece segurança robusta na cadeia de suprimentos, garantindo que os sistemas estejam seguros e livres de violação desde a fábrica até a implementação. Isso aumenta a segurança, a confiabilidade e o desempenho gerais para os clientes da Dell.

Protegendo endpoints com Dell Trusted Devices

Os Dell Trusted Devices integram segurança nos níveis de hardware e firmware para criar sistemas à prova de adulteração.

- **O SafeBIOS** garante a integridade do firmware na inicialização, impedindo alterações não autorizadas de configuração, e verifica a integridade do firmware na inicialização, impedindo a inicialização de sistemas comprometidos.
- **O SafeID** protege as credenciais de autenticação no nível do hardware, impede o acesso não autorizado e protege as credenciais de log-in ao proteger as chaves de autenticação, bloqueando usuários não autorizados.
- **O SafeData** permite a criptografia de ponta a ponta para arquivos confidenciais de negócios, bloqueando tentativas de exfiltração exploratória de dados.

Detecção proativa de ameaças com a CrowdStrike

A CrowdStrike se integra às tecnologias da Dell para fornecer insights em tempo real sobre o comportamento de softwares mal-intencionados.

- **Lógica analítica de detecção de ameaças comportamentais:** Monitora comportamentos de hardware e firmware em busca de sinais de adulteração e detecta atividades incomuns de software para evitar a implementação de malware.
- **Ferramentas de resposta imediata:** A IA isola sistemas comprometidos, impedindo movimentos laterais dentro da rede.
- **Correção de ameaças baseada em IA:** Identifica e isola ativamente ameaças, evitando a disseminação lateral nos sistemas corporativos.
- **Recursos de integração:** Ambientes híbridos e multicloud são protegidos holisticamente com ferramentas da Dell e da CrowdStrike.

Segurança reforçada por meio de soluções de servidor e armazenamento da Dell

A família de servidores Dell PowerEdge incorpora proteção avançada para proteger plataformas de software de missão crítica. Sistemas de armazenamento como o Dell PowerStore oferecem criptografia líder do setor para aplicativos e dados.

- **Firmware de servidor seguro:** Monitora e bloqueia alterações não autorizadas no nível do hardware.
- **Monitoramento de rede isolada:** Detecta anomalias indicativas de adulteração da cadeia de suprimentos.
- **Backups imutáveis:** Protegem os pontos de recuperação mesmo quando o armazenamento primário é comprometido.
- **Cofres de recuperação:** ambientes isolados que protegem contra falhas em cascata iniciadas a partir de sistemas comprometidos.

Abordagens multicamadas para reduzir riscos

A Dell incentiva as empresas a adotar estratégias abrangentes que combinem tecnologia, práticas de pessoal e processos atualizados.

Etapas estratégicas

- **Aumentar a visibilidade da cadeia de suprimentos:** Exige que todos os fornecedores sigam padrões de segurança rigorosos e certifiquem o hardware em todas as etapas.
- **Implementar a criptografia avançada:** Protege dados em todos os níveis usando protocolos avançados, limitando a acessibilidade mesmo em hardware comprometido.
- **Adotar políticas de Zero Trust:** Nenhum dispositivo, aplicativo ou usuário ganha confiança automaticamente sem verificação.
- **Proteger os padrões de codificação:** Colabore com parceiros de software aplicando diretrizes rigorosas para plug-ins, APIs e integrações.
- **Monitorar atividade e realizar auditorias regularmente:** Auditorias de visibilidade frequentes garantem a integridade em serviços de terceiros.
- **Realizar testes regulares:** Implemente testes de invasão e avaliações de firmware para validar continuamente a integridade do dispositivo.
- **Capacitar funcionários:** Treine as equipes para reconhecer componentes ou pacotes que apresentem comportamentos suspeitos.

Como o Dell Professional Services garante a resiliência dos negócios

O Dell Professional Services orienta as empresas na implementação de defesas robustas da cadeia de suprimentos. Equipes de especialistas experientes em segurança cibernética fornecem avaliações, treinamento e estratégias de resposta a ameaças adaptadas às necessidades organizacionais exclusivas.

- **Orientações de implementação:** Alinhe estrategicamente práticas de Zero Trust e de fornecedores auditadas em todos os ambientes de fornecedores.
- **Respostas a incidentes:** Assegure que as empresas se recuperem rapidamente após incidentes mal-intencionados.

Sistemas empresariais preparados para o futuro com a Dell

Os ataques cibernéticos à cadeia de suprimentos exemplificam a sofisticação das ameaças modernas. As empresas precisam de proteção que não apenas previna violações, mas também garanta recuperação rápida quando incidentes ocorrerem. A parceria com a Dell Technologies significa obter acesso a ferramentas de ponta, conhecimento estratégico e uma rede de colaboradores confiáveis.

Dê o próximo passo

Proteja ativos confidenciais e otimize a confiabilidade operacional implementando as melhores práticas fornecidas pela Dell Technologies. Entre em contato hoje para uma consultoria personalizada enquanto se prepara para proteger os recursos vitais dos sistemas da sua empresa.

A Dell Technologies representa confiança, adaptabilidade e inovação à medida que a segurança cibernética da cadeia de suprimentos evolui. O comprometimento de hoje garante o sucesso de amanhã.

Um futuro mais seguro e protegido começa com a Dell Technologies. Confie em nós para proteger o que mais importa.

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

Saiba mais sobre as soluções da Dell

Entre em contato com um especialista da Dell Technologies

Veja mais recursos

Participe da conversa com #HashTag

DELL Technologies