DELL Technologies

Usuários internos mal-intencionados: Fortalecendo a segurança cibernética e a resiliência com a Dell Technologies

A ameaça crescente dos ataques internos mal-intencionados

Ataques internos mal-intencionados se tornaram uma das ameaças mais urgentes à segurança cibernética no cenário empresarial atual. Ao contrário das ameaças externas, os ataques internos mal-intencionados já possuem um certo nível de confiança e acesso dentro de uma organização, tornando suas ações particularmente prejudiciais e difíceis de detectar. Do acesso a dados confidenciais à sabotagem de sistemas, ataques internos podem prejudicar operações críticas e causar graves repercussões financeiras e de reputação.

A Dell Technologies reconhece o perigo crescente representado por esses ataques e desenvolve soluções inovadoras e escaláveis para capacitar empresas a identificar, prevenir e reduzir os riscos de invasores internos mal-intencionados. Ao combinar tecnologia de última geração com serviços liderados por especialistas, a Dell está ajudando as organizações a ficarem à frente dessas ameaças internas.

O que são ataques internos mal-intencionados?

Um ataque interno mal-intencionado ocorre quando um indivíduo dentro de uma organização usa indevidamente seu acesso para comprometer dados, interromper operações ou extrair informações confidenciais para objetivos pessoais, financeiros ou da concorrência. Esse indivíduo pode ser um funcionário, contratado, parceiro ou qualquer pessoa com acesso legítimo aos sistemas e redes da empresa.

Como os ataques internos mal-intencionados funcionam

Os invasores internos mal-intencionados exploram sua posição de confiança para contornar as defesas de segurança tradicionais. As técnicas comuns incluem:

1. **Roubo de dados:** Exfiltração de dados confidenciais de clientes, propriedade intelectual ou registros financeiros.
2. **Sabotagem:** Danificando intencionalmente sistemas de TI para interromper operações comerciais ou manchar a reputação.
3. **Abuso de credenciais:** Uso de credenciais roubadas ou utilizadas incorretamente para aumentar privilégios de acesso ou criar contas fictícias.
4. **Colaboração com invasores externos:** Compartilhamento de acesso ou de informações confidenciais com criminosos cibernéticos externos em troca de ganhos financeiros.

Essa dupla vantagem de confiança e conhecimento interno torna os invasores internos mal-intencionados excepcionalmente perigosos em comparação aos invasores externos.

O impacto nos negócios

O impacto dos ataques internos mal-intencionados é amplo, causando danos que vão além das perdas financeiras. As empresas podem enfrentar consequências como:

Perdas financeiras

O roubo de informações confidenciais, fraudes ou sabotagem podem gerar prejuízos de milhões de dólares em receitas e custos de recuperação.

Disrupção operacional

A sabotagem do sistema ou a destruição de dados pode interromper as operações, resultando em atrasos, oportunidades perdidas e redução da produtividade.

Danos à reputação

Uma violação ou ataque por usuários internos abala a confiança de clientes e investidores, afetando a fidelidade e a percepção de mercado.

Não conformidade regulatória

Em setores específicos, como saúde ou segurança, os ataques internos podem resultar em multas e penalidades pesadas se houver vazamento de dados confidenciais.

Exemplo do mundo real

Em 2020, um prestador de serviços de TI que trabalhava para uma grande instituição financeira excluiu intencionalmente configurações críticas do sistema, causando interrupções na rede por mais de **10 horas**. Esse ato de sabotagem resultou em **milhões** de dólares em perdas financeiras, altos custos de recuperação e danos à reputação. Tais incidentes ilustram o potencial destrutivo de ameaças internas e enfatizam a urgência de medidas robustas de detecção e prevenção.

83%

das organizações relataram pelo menos um ataque interno no último ano

Fonte: 2024: Cybersecurity Insiders' Report

Custos estimados

O custo médio de um incidente relacionado a informações privilegiadas é estimado em **US$ 4,99 milhões** e representa quase **55%** de todas as violações, de acordo com um estudo do Ponemon Institute de 2024. Esse valor representa as despesas de detecção, recuperação e redução, revelando a necessidade crítica das organizações investirem em defesas preventivas contra riscos internos.

Combatendo ataques de usuários internos mal-intencionados com a Dell Technologies

A Dell Technologies oferece um ecossistema abrangente de ferramentas e serviços para combater ameaças internas mal-intencionadas, garantindo que sua organização esteja preparada para o inesperado.

Endpoints seguros com Dell Trusted Devices

Endpoints geralmente servem como pontos de entrada para ameaças internas. Os Dell Trusted Devices integram recursos de segurança de ponta ao hardware para fortalecer endpoints e proteger dados confidenciais.

- **O Dell SafeBIOS** garante a integridade do firmware, impedindo tentativas de manipular as operações do sistema no nível do hardware.
- **O SafeID** protege dados de credenciais, impedindo acesso não autorizado e abuso de credenciais.
- **O SafeData** criptografa dados confidenciais completamente, garantindo que as informações interceptadas ou extraídas permaneçam ilegíveis para invasores internos mal-intencionados.

Ao implementar essas soluções, as organizações podem garantir que seus endpoints estejam protegidos, independentemente de a ameaça ter origem interna ou externa.

Detecção proativa de ameaças com a CrowdStrike

A identificação de ameaças internas requer visibilidade e monitoramento dos comportamentos dos usuários. A CrowdStrike, integrada às soluções da Dell, utiliza inteligência artificial e lógica analítica comportamental para detectar anomalias indicativas de ameaças internas.

Por exemplo, transferências anormais de dados fora do horário comercial ou acessos não autorizados a áreas críticas da rede são indicados imediatamente, facilitando uma resposta rápida. Uma organização de saúde dos EUA recentemente utilizou a detecção proativa de ameaças para identificar e encerrar a tentativa de um funcionário de exfiltrar dados de pacientes, evitando uma violação dispendiosa.

Proteção de dados aprimorada com o Dell PowerProtect

O Dell PowerProtect fornece uma linha de defesa robusta por meio de backups seguros, armazenamento com air gap e cópias imutáveis de dados críticos. Ao garantir que informações confidenciais sejam protegidas contra alteração ou exclusão, os ataques internos que visam a integridade dos dados podem ser ineficazes.

Um exemplo é uma empresa de fabricação que enfrentou um funcionário descontente tentando sabotar arquivos de um projeto. O cofre de recuperação do Dell PowerProtect permitiu que a empresa restaurasse as operações dentro de poucas horas, evitando interrupções e mantendo a continuidade dos negócios.

Recuperação rápida de incidentes com o Dell Professional Services

Quando uma ameaça interna se transforma em um incidente, uma recuperação rápida é essencial. O Dell Professional Services, incluindo recuperação remota de dados e resposta a incidentes, garante que as empresas possam recuperar dados e sistemas rapidamente. Os especialistas da Dell lideram o processo para minimizar o tempo de inatividade e reduzir os impactos.

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

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 rigorosos e análise de tráfego em tempo real em toda a sua infraestrutura.

A importância de uma abordagem de segurança multicamadas

Uma defesa eficaz contra riscos internos requer mais de uma camada de proteção. Implementar uma estratégia de segurança em várias camadas garante que nenhuma vulnerabilidade se torne um ponto fraco. As principais etapas incluem:

Principais etapas para aprimorar a defesa

- **Princípios de Zero Trust:** Verifique continuamente todas as solicitações de acesso e assuma que nenhuma entidade é inerentemente confiável, mesmo dentro do perímetro.
- **Controles de acesso baseados em função (RBAC):** Restrinja o acesso dos funcionários somente aos sistemas e dados necessários para suas funções.
- **Soluções avançadas de criptografia:** Criptografe dados em repouso e em trânsito, neutralizando efetivamente o roubo de dados.
- **Conscientização e treinamento dos funcionários:** Incorpore programas frequentes de conscientização de segurança para evitar a participação acidental em atividades mal-intencionadas.
- **Testes regulares do sistema:** Realize testes de penetração e verificações de vulnerabilidade para garantir que as defesas permaneçam confiáveis.

Essas práticas, reforçadas pelas soluções da Dell, criam uma estrutura de proteção formidável e holística contra invasores internos mal-intencionados.

Fortalecendo as defesas por meio de parcerias estratégicas

Os parceiros da Dell com provedores de segurança cibernética líderes do setor, incluindo a **CrowdStrike** e a **Secureworks**, fortalecem ainda mais suas soluções. A CrowdStrike aprimora a segurança de endpoint e fornece informações valiosas sobre ameaças em indicadores de comprometimento, enquanto a Secureworks oferece serviços de detecção e resposta a ameaças avançadas. Essas colaborações garantem que os clientes da Dell se beneficiem de um ecossistema de tecnologias integradas e de ponta.

Por que escolher a Dell Technologies para a segurança cibernética

A Dell Technologies continua estabelecendo o padrão de excelência em soluções de segurança cibernética multicamadas. As empresas se beneficiam do conhecimento líder do setor da Dell, de parcerias sólidas e do conjunto inovador de produtos que se adaptam ao atual cenário de ameaças em evolução. Desde a segurança de endpoints até a detecção de informações privilegiadas e a recuperação de incidentes, a Dell oferece uma estrutura completa de resiliência que inspira confiança e permite o crescimento.

Construa um futuro resiliente com a Dell Technologies

Proteja sua empresa contra ameaças internas mal-intencionadas com as soluções abrangentes e escaláveis da Dell Technologies. Ao fazer parceria com a Dell, você não está apenas protegendo suas operações, mas também garantindo a continuidade dos negócios, promovendo a confiança do cliente e preparando sua organização para o futuro. Entre em contato conosco para saber mais sobre como implementar defesas proativas hoje mesmo.

A Dell Technologies é sua aliada confiável no combate a ameaças internas, protegendo seus ativos críticos e capacitando sua empresa a prosperar em um ambiente digital dinâmico. Um futuro de segurança é um futuro de sucesso, e começa com a Dell.

Saiba como enfrentar 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