DELL Technologies

Man-in-the-Middle (MITM): Fortalecendo a segurança cibernética e a resiliência com a Dell Technologies

A ameaça crescente dos ataques Man-in-the-Middle (MITM)

Os ataques Man-in-the-Middle (MITM) continuam sendo um dos desafios mais sofisticados e perigosos da segurança cibernética. Esses ataques, em que agentes mal-intencionados interceptam e alteram comunicações privadas sem serem detectados, visam empresas de todos os portes em todos os setores. De plataformas de comércio eletrônico a instituições financeiras, nenhuma organização está imune a esse risco. Os ataques de MITM geralmente abrem caminho para roubo de dados, fraude financeira e danos à reputação, tornando-os um adversário formidável em um cenário cada vez mais digital.

A Dell Technologies entende os desafios únicos que as empresas enfrentam ao se proteger contra essas ameaças avançadas. Ao fornecer soluções de segurança inovadoras e escaláveis, a Dell capacita as organizações a neutralizar ameaças MITM, proteger ativos e manter a integridade dos negócios.

O que é um ataque Man-in-the-Middle (MITM)?

Um ataque Man-in-the-Middle (MITM) acontece quando um criminoso cibernético intercepta secretamente comunicações entre duas partes, como entre um funcionário e um servidor corporativo ou um cliente e um site empresarial. O objetivo do invasor pode variar, desde roubar dados confidenciais até manipular comunicações para fins mal-intencionados, mas o resultado é o mesmo: uma quebra de confiança e segurança.

Técnicas comuns de MITM

Alguns dos métodos mais comuns usados pelos invasores incluem o seguinte:

Espionagem de Wi-Fi: Criminosos cibernéticos exploram redes Wi-Fi públicas desprotegidas ou comprometidas para interceptar comunicações.

Falsificação de DNS: Invasores redirecionam usuários para sites fraudulentos, adulterando registros de DNS e coletando informações confidenciais sem suspeitar.

Sequestro de sessão: Ao confiscar credenciais de sessão ativa, os invasores obtêm acesso não autorizado a contas privadas.

SSL Stripping: Essa técnica rebaixa conexões HTTPS seguras para HTTP vulneráveis, expondo informações confidenciais.

Essa adaptabilidade torna os ataques MITM particularmente prejudiciais, pois eles exploram transações e interações comerciais cotidianas que parecem legítimas à primeira vista.

O impacto nos negócios

Os efeitos cascata de um ataque MITM vão muito além do incidente imediato. Algumas das consequências mais prejudiciais incluem:

Receita perdida

Credenciais roubadas e operações comprometidas geralmente resultam em encargos financeiros que vão desde perdas diretas até custos de recuperação.

Contratempos operacionais

O tempo e os recursos gastos na resolução de um ataque prejudicam funções de negócios essenciais, impactando a produtividade e o crescimento.

Desgaste da confiança

A confiança do cliente pode falhar rapidamente quando suas informações pessoais são violadas, causando danos à reputação a longo prazo.

Impacto regulatório

Empresas que operam em setores com rigorosos requisitos de conformidade podem enfrentar multas ou sanções após uma violação de dados.

Exemplo do mundo real

Um caso alarmante envolveu uma empresa global de varejo cuja plataforma de pagamento on-line não criptografada foi vítima de um ataque de SSL Stripping. O invasor interceptou informações de cartão de crédito dos clientes durante a finalização da compra. Por meio da rápida detecção e de medidas estratégicas de segurança, incluindo as ferramentas de proteção de endpoints da Dell, a empresa conseguiu conter o ataque e reduzir os danos de longo prazo. Este cenário destaca os riscos imediatos e a necessidade crítica de defesas em camadas.

35,9 bilhões

de violações de dados conhecidas globalmente

Fonte: Maio de 2024: Relatório da PureWL

Combatendo ataques de MITM com a Dell Technologies

A Dell Technologies equipa organizações com ferramentas abrangentes e inovadoras, desenvolvidas para impedir riscos de MITM antes que eles causem danos.

Endpoints seguros com Dell Trusted Devices

Os endpoints são pontos comuns de origem de ameaças MITM, tornando sua proteção uma prioridade. Os dispositivos confiáveis da Dell incorporam segurança de última geração diretamente no hardware. Por exemplo:

- **O Dell SafeBIOS** garante que a integridade do sistema seja protegida contra adulterações não autorizadas na sequência de boot.
- **O SafeID** adiciona outra camada de proteção ao proteger os dados de autenticação do usuário, criando uma fortaleza contra roubo de credenciais.
- **O Dell SafeData** oferece criptografia completa que protege informações confidenciais dentro e fora dos firewalls corporativos, deixando ilegíveis os dados interceptados.

Esses recursos foram implementados em empresas globais para impor confiança em sistemas de endpoint. Por exemplo, uma empresa multinacional de fabricação usou os Dell Trusted Devices para defender sua força de trabalho remota de ataques MITM direcionados a notebooks corporativos, garantindo conexões seguras mesmo durante cenários de viagens de alto risco.

Detecção avançada com a CrowdStrike

Detectar e responder a ameaças MITM em tempo real é crucial. A CrowdStrike, integrada ao ecossistema da Dell, utiliza inteligência artificial e lógica analítica comportamental para monitorar e neutralizar atividades suspeitas. O monitoramento contínuo garante proteção em ambientes híbridos, onde as ameaças geralmente se escondem. Ao identificar anomalias de forma proativa, as empresas podem eliminar possíveis tentativas de MITM antes que os danos ocorram.

Por exemplo, usando detecção avançada, uma instituição financeira detectou e reduziu com sucesso uma invasão em seu portal voltado ao cliente. A IA da plataforma identificou atividade de rede incomum indicativa de SSL Stripping, permitindo correção imediata.

Proteção de dados reforçada com o Dell PowerProtect

Mesmo organizações com defesas avançadas podem sofrer violações. É aí que o Dell PowerProtect entra. Com recursos como imutabilidade e armazenamento com air gap, ele protege dados de negócios críticos contra alterações, destruição ou acesso durante um ataque. O cofre do PowerProtect Cyber Recovery oferece segurança adicional ao isolar dados confidenciais de redes primárias, garantindo que, mesmo nos piores cenários, as informações confidenciais permaneçam intactas e recuperáveis.

Essa tecnologia foi fundamental para uma organização de saúde que enfrentou um ataque de falsificação de DNS. Ao aproveitar os backups imutáveis e o cofre de recuperação do PowerProtect, a organização restaurou as operações rapidamente, sem perda de dados.

Serviços de recuperação e resposta rápida

O Data Protection Services da Dell complementa suas tecnologias oferecendo recuperação rápida e liderada por especialistas em caso de violação. Da recuperação remota de dados à resposta a incidentes, essas soluções reduzem o tempo de inatividade e minimizam a interrupção operacional. Quando cada segundo conta, ter um parceiro confiável garante que as organizações possam se recuperar com confiança.

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.

Fortalecendo a segurança com uma abordagem multicamada

Para combater totalmente os ataques MITM, as organizações devem implementar uma estratégia de segurança multifacetada. A Dell Technologies enfatiza estas etapas práticas:

- **Adote os princípios de Zero Trust:** Verifique todas as atividades e o acesso dos usuários em cada ponto, independentemente de se originarem dentro ou fora da rede corporativa.
- **Usar criptografia avançada:** Criptografia completa para todas as comunicações garante que os dados interceptados se tornem inutilizáveis para os invasores.
- **Implementar autenticação baseada em vários fatores (MFA):** A MFA adiciona camadas de autenticação aos sistemas, reduzindo significativamente as vulnerabilidades de acesso não autorizado.
- **Capacitar funcionários:** Crie uma força de trabalho mais vigilante, destacando riscos como esquemas de phishing, uso suspeito de Wi-Fi e links não verificados.
- **Testes regulares do sistema:** Testes de violação e atualizações frequentes ajudam a identificar vulnerabilidades e garantir que as defesas permaneçam atualizadas.

As ofertas de segurança holística da Dell, combinadas com essas práticas, criam uma defesa formidável e adaptável contra ameaças em evolução.

O valor das parcerias estratégicas

A colaboração da Dell Technologies com empresas líderes em segurança cibernética, como a CrowdStrike e a Secureworks, fortalece ainda mais suas ofertas. A integração da experiência nessas parcerias permite que a Dell aborde todos os vetores de ataque possíveis. A CrowdStrike, por exemplo, aprimora a proteção de endpoints ao enriquecer as plataformas da Dell com inteligência contra ameaças, enquanto a Secureworks fornece insights práticos sobre riscos em evolução, garantindo preparação e adaptação contínuas.

A vantagem da Dell Technologies

Escolher a Dell Technologies significa fazer parceria com um líder confiável em inovação em segurança cibernética. Seja por meio da proteção de endpoints, da recuperação de dados ou de parcerias colaborativas, as soluções completas da Dell permitem que as organizações se mantenham sempre à frente dos invasores.

Proteja sua empresa, mantenha a confiança do cliente e prepare suas operações para o futuro com as soluções abrangentes de MITM da Dell. Entre em contato conosco hoje mesmo para começar a construir um futuro resiliente e seguro para seus negócios.

Ao fazer parceria com a Dell Technologies, você assume uma postura ativa contra ameaças cibernéticas, criando confiança duradoura com clientes e partes interessadas e garantindo o sucesso operacional em um mundo digital cada vez mais inseguro. Um futuro mais seguro 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