O ZScaler divulga a violação de dados após o compromisso da instância

Data: 2025-09-02 05:12:44

Autor: Inteligência Against Invaders

A empresa de segurança cibernética ZSCALER divulgou uma violação de dados que afeta as informações de contato do cliente depois que atores não autorizados obtiveram acesso ao banco de dados do Salesforce da empresa por meio de credenciais de aplicativos de terceiros comprometidos. A violação se originou de uma campanha mais ampla direcionada à Salesloft Drift, uma plataforma de automação de marketing que se integra aos bancos de dados do Salesforce para gerenciar leads e relacionamentos com os clientes.

Os cibercriminosos roubaram com sucesso [Oauth Tokens](#) Da Salesloft Drift, concedendo a eles acesso não autorizado a instâncias do Salesforce conectadas em várias organizações, incluindo o ZScaler.

O provedor de segurança em nuvem enfatizou que o incidente estava confinado ao seu ambiente Salesforce e não comprometeu nenhum dos principais produtos, serviços ou sistemas de infraestrutura subjacentes do ZSCALER que protegem milhares de clientes corporativos em todo o mundo.

Escopo de exposição aos dados

De acordo com a investigação do ZScaler, o acesso não autorizado foi limitado a informações de contato comercial e conteúdo específico do Salesforce.

Os dados comprometidos incluíram nomes de clientes, endereços de e-mail comercial, títulos de emprego, números de telefone, detalhes da localização regional e informações de licenciamento de produtos ZScaler.

Além disso, o conteúdo simples de texto de certos casos de suporte ao cliente foi acessado, embora a empresa tenha confirmado que anexos, arquivos e imagens permanecem seguros.

O ZScaler afirmou que sua extensa investigação não encontrou evidências de uso indevido de dados após a violação.

No entanto, a empresa reconheceu que as informações de contato expostas poderiam ser potencialmente alavancadas para [ataques de phishing](#) ou tentativas de engenharia social direcionadas aos clientes afetados.

O ZScaler respondeu imediatamente após o aprendizado do incidente, tomando várias medidas de proteção para conter a violação e impedir ocorrências futuras.

A empresa revogou o acesso da Salesloft Drift ao seu ambiente Salesforce e girou outros tokens de acesso à API como medida de precaução.

Trabalhando em estreita colaboração com o Salesforce, o ZScaler lançou uma investigação abrangente para avaliar o escopo completo do incidente, implementando salvaguardas adicionais e fortalecendo os protocolos de segurança.

A empresa também iniciou uma revisão de gerenciamento de riscos de terceiros de todas as relações de fornecedores e os procedimentos aprimorados de autenticação de clientes para interações de suporte.

O incidente destaca os riscos crescentes associados a integrações de terceiros em ambientes corporativos.

O compromisso da Salesloft Drift afetou vários clientes do Salesforce além do ZScaler, demonstrando como os ataques da cadeia de suprimentos podem cascata em várias organizações por meio de provedores de serviços compartilhados.

[ZScaler](#) aconselhou os clientes a permanecerem vigilantes contra possíveis tentativas de phishing que poderiam explorar as informações de contato expostas.

A Companhia enfatizou que a equipe legítima de suporte ao ZScaler nunca solicitará credenciais de autenticação por meio de comunicações não solicitadas e instou os clientes a verificar a fonte de solicitações de contato inesperadas.

Os clientes que sofrem de atividades suspeitas ou exigindo suporte adicional podem entrar em contato com o ZScaler através de canais oficiais em help.zscaler.com.

A Companhia se comprometeu a fornecer atualizações contínuas à medida que a investigação progride e quaisquer novos desenvolvimentos emergem.

Essa violação serve como outro lembrete da importância crítica de proteger integrações de terceiros e manter programas robustos de gerenciamento de riscos de fornecedores no ambiente de negócios interconectado de hoje.

Encontre esta história interessante! Siga -nos [LinkedIn](#) X Para obter mais atualizações instantâneas.