LNER revela que o ataque à cadeia de suprimentos comprometeu as infor

Data: 2025-09-11 09:30:00

Autor: Inteligência Against Invaders

A operadora de uma das linhas ferroviárias mais movimentadas do Reino Unido admitiu que um terceiro não autorizado acessou os detalhes do cliente por meio de um fornecedor.

A LNER, empresa estatal que administra os serviços da costa leste entre Londres e a Escócia, revelou o incidente em uma atualização online ontem.

“Fomos informados do acesso não autorizado a arquivos gerenciados por um fornecedor terceirizado, que envolve detalhes de contato do cliente e algumas informações sobre viagens anteriores”, disse.

“É importante ressaltar que nenhuma informação bancária, de cartão de pagamento ou senha foi afetada.”

No entanto, a operadora de trem alertou que informações comprometidas podem ser usadas para atingir clientes em ataques subsequentes.

“Por favor, tenha cuidado com comunicações não solicitadas, especialmente aquelas que pedem informações pessoais. Em caso de dúvida, não responda”, pediu.

Leia mais sobre as ameaças que afetam o setor ferroviário: Cibercriminosos invadem o Wi-Fi da rede ferroviária do Reino Unido

Os avisos do LNER foram ecoados por especialistas em segurança.

“Os dados expostos na violação do LNER, embora não sejam de contexto crítico de segurança, ainda podem ser usados para gerar documentos de phishing atraentes e outros ataques contra a identidade de um usuário”, disse o analista sênior de operações de segurança da Huntress, Michael Tigges.

“Incidentes como esses são um lembrete gritante de que, embora a organização principal possa proteger nossos dados, terceiros em todo o mundo lidam constantemente com dados e informações pessoais no curso regular de seus negócios.”

Ele instou as empresas a realizar exercícios regulares de mesa, bem como descoberta de dados, para entender onde as informações confidenciais fluem para fora da organização e como elas são

protegidas.

“Os usuários finais devem considerar fortalecer suas identidades (e-mails e informações pessoais) com sistemas de detecção e resposta a ameaças de identidade para ajudar a detectar ataques que possam transformar as informações roubadas em armas”, acrescentou Tigges.

Como nenhuma senha foi roubada no incidente, o LNER não está redefinindo as credenciais do cliente, embora tenha lembrado que “é sempre uma boa prática manter uma senha segura e alterar as senhas regularmente”.

Em um discurso em Londres ontem, o ministro da Segurança, Dan Jarvis, chamou várias iniciativas do governo destinadas a reprimir ameaças cibernéticas e de fraude.

“Estamos aumentando os poderes da polícia por meio do Projeto de Lei de Crime e Policiamento, para que a aplicação da lei possa suspender endereços IP e nomes de domínio usados para facilitar crimes graves”, disse ele.

“E estou impulsionando em todo o governo o novo pacote de medidas legislativas que pretendemos introduzir no próximo ano para proteger as empresas do Reino Unido contra ransomware.”

Crédito da imagem: Bradley Caslin / Shutterstock.com