
Renault e Dacia UK alertam para violação de dados que afeta clientes

Data: 2025-10-03 16:13:06

Autor: Inteligência Against Invaders

Os clientes da Renault e da Dacia no Reino Unido foram notificados de que informações confidenciais que compartilharam com a montadora foram comprometidas após uma violação de dados em um fornecedor terceirizado.

Com uma receita de mais de US\$ 55 bilhões, a montadora francesa tem 170.000 funcionários e uma produção anual de 2,2 milhões de veículos. A Dacia é uma marca subsidiária que oferece veículos confiáveis a um preço acessível.

Ontem, ambas as marcas informaram os clientes [[1](#), [2](#)] que eles foram afetados pelo incidente de segurança cibernética que ocorreu em um terceiro não identificado.

“Lamentamos informar sobre um ataque cibernético a um de nossos fornecedores terceirizados, levando à retirada de dados pessoais de alguns clientes da Renault UK de um de seus sistemas”, diz o aviso.

As informações que foram expostas incluem os seguintes tipos de dados:

- Nome completo
- Gênero
- Telefone
- Endereço eletrônico
- Endereço postal
- Número de identificação do veículo
- Número de matrícula do veículo

Um invasor pode usar esse tipo de informação para direcionar usuários em campanhas de phishing, golpes e outras formas de engenharia social.

A notificação da montadora destaca que informações bancárias ou financeiras não foram expostas devido a este incidente.

[IMAGEM REMOVIDA] ataque cibernético à Jaguar Land Rover no Reino Unido, que teve um impacto significativo nas operações, pois a montadora foi forçada a interromper a produção de [quase um mês](#).

Esse ataque também envolveu [Roubo de dados](#), embora não tenham sido divulgados publicamente muitos pormenores, e tiveram um impacto tal que a JLR teve de aceitar uma garantia do Governo do

Reino Unido [Empréstimo de £ 1,5 bilhão](#) para restaurar sua cadeia de suprimentos.

[\[IMAGEM REMOVIDA\]](#)

-

[O Evento de Validação de Segurança do Ano: O Picus BAS Summit](#)

Junte-se ao **Cúpula de Simulação de Violação e Ataque** e experimente o **Futuro da validação de segurança**. Ouça os principais especialistas e veja como **BAS alimentado por IA** está transformando a simulação de violação e ataque.

Não perca o evento que moldará o futuro da sua estratégia de segurança