
Gigante japonesa da cerveja Asahi confirma ataque de ransomware - Agai

Data: 2025-10-03 17:25:36

Autor: Inteligência Against Invaders

A gigante japonesa de fabricação de cerveja Asahi divulgou hoje que um ataque de ransomware causou as interrupções de TI que a forçaram a fechar fábricas esta semana.

A holding de bebidas com sede em Tóquio é a maior cervejaria do Japão, empregando 30.000 pessoas e produzindo 100 milhões de hectolitros de bebidas.

A empresa também possui as marcas Peroni, Pilsner Urquell, Grolsch e Fullers, e registrou uma receita anual de quase US\$ 20 bilhões em 2024.

A Asahi revelou em um comunicado hoje que um [ataque cibernético divulgado na segunda-feira](#) levou à implantação de ransomware em sua rede e que uma investigação subsequente também encontrou evidências de roubo de dados de dispositivos comprometidos.

“A Asahi Group Holdings, Ltd. está atualmente enfrentando uma falha no sistema causada por um ataque cibernético, afetando as operações no Japão”, disse a empresa na segunda-feira.

Embora a Asahi tenha confirmado que um ataque de ransomware atingiu seus sistemas, nenhuma operação de ransomware reivindicou a responsabilidade pelo ataque, o que implica que a empresa não respondeu às demandas dos invasores, ainda está negociando ou já pagou um resgate.

“Ao detectar o incidente, estabelecemos uma Sede de Resposta a Emergências para investigar o incidente, por meio da qual confirmamos que nossos servidores foram alvo de um ataque de ransomware”, disse a empresa hoje.

“Investigações subsequentes confirmaram vestígios sugerindo uma potencial transferência não autorizada de dados. Estamos conduzindo uma investigação para determinar a natureza e o escopo das informações que podem ter sido sujeitas a transferência não autorizada.”

O BleepingComputer ainda não recebeu uma resposta depois de entrar em contato com a Asahi após a divulgação inicial para perguntar se algum grupo de crimes cibernéticos exigiu um resgate e se os sistemas na rede da empresa foram criptografados.

De acordo com Asahi, embora o ataque de ransomware tenha afetado apenas fábricas no Japão, ele forçou a empresa a mudar para o processamento e envio manual de pedidos porque seus “processos de pedidos e remessas baseados no sistema permanecem suspensos”.

“Embora não possamos fornecer um cronograma claro para recuperação no momento, nossa Sede de Resposta a Emergências está trabalhando em colaboração com especialistas externos em segurança cibernética para restaurar o sistema o mais rápido possível. O escopo da interrupção do

sistema está atualmente limitado ao Japão”, observou.

[\[IMAGEM REMOVIDA\]](#)

-

[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