# No Reino Unido, ICO multa empresa que sofreu ataque ransomware em £4,4 milhões por não adotar medidas de segurança adequadas à proteção de dados pessoais

**13.12.2022 2 minutos de leitura**


**Autores**

**Felipe Palhares**

**Fernanda Villela**


**Áreas relacionadas**

Proteção de Dados e Cybersecurity

**Assuntos**

Proteção de Dados e Cybersecurity | Felipe Palhares | Segurança Cibernética | Ransomware | Internet

No dia 24 de outubro, o *Information Commissioner's Office* (ICO), autoridade de proteção de dados do Reino Unido, multou uma companhia no valor de £4,4 milhões por não cumprir com requisitos de segurança para a proteção de dados. Este descumprimento resultou em vulnerabilidades exploradas num ataque *ransomware* que afetou cerca de 113 mil dados pessoais.

No dia 30 de março de 2020, um e-mail de *phishing* foi enviado a dois empregados da companhia como se fosse "urgente". Dois dias depois, o arquivo ZIP do e-mail foi baixado por um empregado, o que resultou na instalação de um *malware* em seu dispositivo. Então, o *hacker* obteve acesso remoto e passou a comprometer outros sistemas, incluindo servidores que continham dados pessoais de 113 mil empregados e ex-empregados da companhia, os quais foram encriptados e ficaram inacessíveis durante cerca de 2 meses. O *ransomware* foi identificado 1 mês depois, logo sendo notificado ao ICO.

Em sua decisão, o ICO concluiu que a companhia não adotou medidas técnicas e organizacionais de segurança da informação adequadas a garantir a confidencialidade, integridade e disponibilidade dos dados pessoais. Em sua decisão, apontaram-se diversos fatores:

- A companhia não implementava de forma efetiva suas políticas e procedimentos internos de proteção de dados;
- A companhia adotava sistemas operacionais e antivírus desatualizados;
- Um dos empregados que recebeu o e-mail de *phishing* não havia participado dos treinamentos da companhia sobre proteção de dados;
- Logo após o incidente, o sistema de *endpoint protection* da companhia removeu apenas alguns dos *malwares*, notificando a equipe de segurança da informação. Contudo, nenhuma outra investigação foi realizada pela companhia; e
- Havia 280 usuários registrados com contas de administradores, das quais 12 foram exploradas pelo *hacker*. Tais contas possuíam permissões amplas para gerenciar estações de trabalho e servidores.

**Para acessar a decisão do ICO, clique aqui.**

› PROFISSIONAIS

# Profissionais que aliam visão jurídica e visão de mercado

**Felipe Palhares**

**Fernanda Villela**