Capgemini, empresa de tecnologia da informação, é condenada a indenizar US$6,5 milhões por perdas de contratante após incidente de segurança

03.01.2023 3 minutos de leitura

Autores

Felipe Palhares

Fernanda Villela

Áreas relacionadas

Proteção de Dados e Cybersecurity

Assuntos

Proteção de Dados e Cybersecurity | Felipe Palhares

No dia 9 de dezembro, a *High Court of the Republic of Singapore* (Corte) decidiu que a Capgemini, empresa prestadora de serviços de tecnologia da informação, seria a responsável por indenizar a Razer, empresa de sistemas e periféricos de jogos. A indenização, que atingiu o montante total de US$6,5 milhões, foi pautada nos prejuízos sofridos pela Razer devido a um vazamento de dados dos seus consumidores.

1. Projeto Fênix

Em 2018, a Razer deu início ao "Projeto Fênix" a fim de atualizar sua plataforma de *e-commerce*, o que incluía sua integração com aplicações de terceiros utilizadas pela Razer por meio de interfaces de programação de aplicações (APIs). APIs são mecanismos que permitem a interação entre duas diferentes aplicações ou *softwares*. No caso, a equipe comercial da Razer desejava acessar dados de consumidores contidos nos canais de *e-commerce*. Antes da integração de API, cópias dos dados eram transferidas para uma outra base de dados. Posteriormente, a API permitiu a transferência direta dos dados à nova base, integrando-a aos canais de *e-commerce* diretamente.

Em março de 2019, a Capgemini foi contratada para apoiar a integração das APIs. No mesmo mês, ambas as empresas também firmaram um contrato para o compartilhamento de dados pessoais (*data processing agreement* – DPA).

Entre 2019 e 2020, a Capgemini recomendou à Razer a instalação e integração de um conjunto de APIs em seu ecossistema de tecnologia da informação. Dentre outros, a Capgemini seria responsável por configurar tais APIs para disponibilizar uma série de dados de consumidores à equipe de *e-commerce* da Razer.

2. Incidente de segurança

Em junho de 2020, um gerente de projetos da Razer teve problemas para acessar um servidor. Então, a Capgemini, como prestadora de serviços de tecnologia da informação, foi acionada para auxiliá-lo. Para atender ao chamado, foi enviado um colaborador que detinha credenciais de administrador do servidor em questão, as quais lhe permitiam acessar e modificar suas configurações de segurança.

Em agosto de 2020, um terceiro informou à Razer "um alerta de segurança" e afirmou que havia identificado "uma base de dados desprotegida e disponível publicamente que parece integrar a infraestrutura da Razer". De acordo com o terceiro, a base de dados incluía "detalhes de consumidores, e-mails, e muito mais".

Todavia, a Razer respondeu-lhe que estava trocando de *bounty program*, isto é, um programa que recompensa terceiros por identificarem vulnerabilidades cibernéticas nos sistemas de empresas, pedindo-lhe que aguardasse a mudança de programa para ser recompensado. Então, o terceiro divulgou o incidente de segurança na internet, o qual recebeu ampla cobertura da imprensa.

No curso da investigação forense foi possível averiguar que o colaborador da Capgemini havia desativado as configurações de segurança de uma das aplicações da Razer, fato posteriormente admitido pelo próprio funcionário. Foi justamente a desconfiguração dos mecanismos de segurança que expôs os dados de consumidores publicamente, sem qualquer proteção.

3. Indenização

A Corte concluiu que a Capgemini violou tanto o contrato de prestação de serviços quanto o DPA celebrados com a Razer. Nos documentos constavam cláusulas de indenização em casos de violações das obrigações estipuladas no objeto contratual.

Além disso, a Corte considerou que a Capgemini foi contratada devido às suas habilidades específicas e *expertise* para realizar trabalhos de integração de APIs, o que resulta em um ônus maior à Capgemini.

De todo o montante, US$6,1 milhões representam os lucros cessantes da Razer pela perda de vendas de sistemas e periféricos de jogos, consequência dos danos reputacionais sofridos devido à cobertura de imprensa negativa após o incidente de segurança.

Para acessar a decisão da *High Court of the Republic of Singapore*, clique aqui.

>>> Este artigo foi escrito por nossos profissionais da área de Proteção de Dados e Cybersecurity: Felipe Palhares, Fernanda Villela, Bárbara Iszlaji e Arthur Pichelli Ueda.

› PROFISSIONAIS

Profissionais que aliam visão jurídica e visão de mercado

Felipe Palhares

Fernanda Villela