11200 Rockville Pike, Suite 220 Rockville, MD 20852 | **Phone**: 301-984-7400 | **Fax**: 301-984-7401
Web: www.asmed.com | **E-mail**: info@asmed.com

High Technology Sector

Source: Deloitte Report

Case 3

Vengeful hacktivists force a leading online platform to shut down for more than a month

Organization

A very large technology company that sells products all around the world and operates a popular online platform.

Scenario

The online platform, which has millions of users, was attacked by a hacktivist group with a grudge against the company. The hackers managed to steal more than 70 million user names and passwords, as well as credit card information in multiple attacks spanning months. In the wake of the attack, the company was forced to temporarily shut down its online service, denying access to users for more than a month.

Attackers and motivation

Prior to the attack, the company had made some decisions in a public case that did not sit well with a particular group of clever hackers. This hacktivist group sought revenge by hitting the company with a very impactful attack.

Techniques used

The initial attack vector the hackers used to infiltrate the company's network is not publicly known. What is known however is that the attackers spent a long time in the company's internal network. During this time they discovered a number of vulnerabilities that could be easily exploited. Most likely they used a SQL injection attack against the online platform's internet-facing servers to steal data from sensitive databases.

Business impact

The company lost personal and credit card information for more than 70 million users. Also, because the attackers were so deeply nested in the internal network, the company decided to close down the online platform for multiple months resulting in major financial losses. Customers were later compensated for the downtime, costing the company even more money. What's more, the breach was reported in the news globally, badly damaging the organization's reputation.