COMELEC data breach (2016) Case Study

Commission on Elections (COMELEC)

SQL injection attack

- SQL injection is a type of web application security vulnerability that allows an attacker to execute malicious SQL statements to manipulate a web application's database.
- COMELEC data breach (2016): The website of the Commission on Elections (COMELEC) was hacked and personal information of millions of Filipino voters was leaked online.
- The attackers exploited vulnerabilities in the COMELEC website and used SQL injection techniques to gain access to the database containing voter information.
- The stolen data included personal information such as full names, addresses, birth dates, and passport numbers.

Company description:

- COMELEC is the Commission on Elections in the Philippines, responsible for administering and supervising elections in the country.

Summary:

- In March 2016, the Philippine Commission on Elections (COMELEC) suffered a data breach that exposed the personal information of 55 million registered voters.
- The attackers behind the breach were a group of hackers known as "LulzSec Pilipinas," who claimed responsibility for the attack.
- The attackers exploited vulnerabilities in the COMELEC website and used SQL injection techniques to gain access to the database containing voter information.
- The stolen data included personal information such as full names, addresses, birth dates, and passport numbers.
- The attackers also leaked a portion of the stolen data online, making it publicly accessible.
- The incident was considered one of the largest government-related data breaches in history, and raised concerns about the security of government systems in the Philippines.

Timeline

COMELEC data breach (2016)Attack

1. March 27, 2016: The COMELEC website is defaced by a hacker group, claiming to be from Anonymous Philippines.
2. March 31, 2016: A hacker claiming to be part of Anonymous Philippines posts a link to a COMELEC database dump containing voter information of millions of Filipinos.
3. April 4, 2016: COMELEC confirms the data breach and announces that it is conducting an investigation.
4. April 20, 2016: The National Bureau of Investigation (NBI) arrests a suspect believed to be involved in the data breach.
5. August 12, 2016: The Department of Justice (DOJ) indicts the arrested suspect, who is identified as a 23-year-old IT graduate.
6. March 29, 2018: The DOJ convicts the suspect for violating the Cybercrime Prevention Act of 2012 and imposes a penalty of imprisonment for up to six years.

Vulnerabilities

The vulnerabilities in the COMELEC data breach include the use of weak passwords, outdated software, lack of encryption, and the absence of a comprehensive cybersecurity plan.

Use of outdated and vulnerable software:

- The COMELEC website was running on an outdated version of the Content Management System (CMS) Joomla, which had several known vulnerabilities that had not been patched.

Weak password policies:

- Some accounts having passwords as simple as "password" or "12345"

Insufficient data protection:

- Database was not properly protected, as evidenced by the lack of encryption and the storage of sensitive information, such as passport numbers, in plain text.

Poor incident response planning:

- The COMELEC IT team did not have a proper incident response plan in place

Costs

- Comelec spent PHP 1.2 billion (USD 23 million) to address the data breach, including investigation, system upgrades, and free credit monitoring for affected individuals.
- 55 million voters' personal information was exposed, including full names, addresses, birth dates, and passport details, which can be used for identity theft, fraud, and other cybercrimes.
- Hackers sold the stolen data on the dark web, potentially earning millions of pesos from buyers.
- Comelec officials faced legal and political backlash for the breach, including calls for resignation and charges for negligence and violation of data privacy laws.
- The incident damaged the reputation of Comelec and the Philippine government, as well as eroded public trust in the electoral system.

Prevention

- Regularly conduct security audits and risk assessments to identify vulnerabilities and mitigate them.
- Regularly conduct security audits and risk assessments to identify vulnerabilities and mitigate them.
- Encrypt sensitive data both in transit and at rest to protect it from unauthorized access.
- Train employees on cybersecurity best practices and ensure that they are aware of the risks and consequences of a data breach.
- Implement intrusion detection and prevention systems to monitor for and respond to potential cyberattacks.
- Have an incident response plan in place to quickly and effectively respond to a data breach if it occurs.