Case Study

Data Breach and Unauthorized Access

Prime company: National Public Data

Other affected parties:

- Consumers
- Jericho Pictures Inc
- Various Businesses

Attack Category: Data Breach and Unauthorized Access

1. Description

This category refers to unauthorized individuals gaining access to sensitive, personal, or financial information stored by a company. In the case of National Public Data, a third-party actor gained unauthorized access to their database.

2. Statistic

Data breaches continue to grow, with 2.9 billion personal records potentially exposed in this breach, showing the extent and severity of the issue in the background check industry. Sources for this information include CNBC, USA today and the Washington Post.

Company Description and Breach Summary

Company Description

National Public Data is a background check company owned by Jerico Pictures Inc. It gathers data, sometimes without consumer consent, by scraping public information and providing this data for various checks.

Breach Summary

- A breach potentially exposed up to 2.9 billion personal records, including Social Security numbers, names, addresses, and more.

- While the company reported 1.3 million records exposed, the lawsuit alleges a much larger figure.

- The breach is said to have occurred between December 2023 and April 2024.

Timeline

1. **December 2023** - Third-party actors gained access to the National Public Data systems.
2. **April 2024** - Possible leaks of sensitive data.
3. **July 2024** - The breach is publicly revealed.
4. **August 2024** - Lawsuit filed alleging 2.9 billion records exposed.
5. **September 2024** - National Public Data files official breach notice, reporting 1.3 million records.
6. **Ongoing** - Investigation and legal actions continue.

Vulnerabilities

The National Public Data breach exposed critical weaknesses in how the company managed and protected sensitive information. This breach highlights the vulnerabilities associated with companies handling large volumes of personal data, especially those that collect such data through scraping public information without stringent security controls.

Vulnerability 1

Lack of secure encryption for sensitive personal data.

Sensitive information such as Social Security numbers and other personal identifiers were likely not adequately encrypted, making it easier for unauthorized individuals to access and exploit the data once a breach occurred.

Vulnerability 2

Inadequate monitoring of system access.

The breach went undetected for several months, indicating weak monitoring systems. Early detection could have minimized the exposure window, but inadequate monitoring allowed bad actors to access and possibly exfiltrate data over an extended period.

Vulnerability 3

Failure to adhere to proper cybersecurity regulations and protocols for protecting public data.

The company's systems appeared to have insufficient restrictions on who could access or retrieve personal data, creating an environment where unauthorized access by third parties could occur. This lack of access controls makes it easier for external threats to penetrate systems.

Vulnerability 4

Delayed detection of the breach, which led to extensive data exposure over several months.

National Public Data did not seem to follow critical cybersecurity regulations and standards (e.g., GDPR, CCPA), especially in protecting consumer data. This failure not only left the company vulnerable to breaches but also exposed it to legal repercussions.

Costs and Prevention

Costs

- 1- Legal expenses related to the class action lawsuit.
- 2- Potential fines and penalties if found negligent in securing the data.
- 3- Reputational damage, leading to loss of business and consumer trust.

Prevention

- 1- Implement stronger encryption and data protection standards.
- 2- Regularly audit system access and perform vulnerability assessments.
- 3- Educate employees on cybersecurity best practices to minimize risks.
- 4- Adopt multi-factor authentication and monitor dark web activity for breached data.