Overview of Top CyberSecurity Breaches In India

Impacts, Methods & Recommendations on Mitigation Techniques

FireCompass

Overview

Indian enterprises are rapidly moving to the digital realm, which makes it extremely important to have a well-defined cybersecurity strategy. This will help flush out many risks and minimise the impact of any possible breaches.

To protect ourselves, we need to also look into the attacks that were carried out in the past, what kind of information was sought out for, attack patterns, common vulnerabilities that were targeted etc.

This report on the cyber-attacks on various Indian organisations along recommendations on top mitigation techniques will give us an idea about what to focus on.

There have been a number of hack attacks reported in India and around the world in the recent past, hackers get smarter with every hack and so should our security.

Top Cyber Security Breaches

Government Sectors

1. **Telecom Regulatory Authority of India (TRAI)** - The website was brought down by a hacker group.

   Impact: Website downtime, service made unavailable using DDOS attack.

   Source: The Indian Express

2. **Indian Army –** the website was brought down and defaced with inappropriate advertisements, some sensitive data was inaccessible and was feared to be stolen.

   Impact: Information inaccessible and officer details may be stolen, website defacement.

   Source: The Times of India

3. **Jawaharlal Nehru University (JNU) library** - website was compromised to warn the 'anti-nationals' and 'Traitors'.

   Impact: Website defacement

   Source: The Indian Express

4. **Orissa University of Agriculture and Technology (OUAT)** – The official website was hacked.

   Impact: Not disclosed.

   Source: The Times of India

5. **Indian Space Research Organisation (ISRO)** – The home page of ISROS's commercial arm Antrix was hacked.

   Impact: Not disclosed.

   Source: The Hindu

6. **Kerala Government website –** Official website was defaced and carried a message.

   Impact: Defacement.

   Source: The Hindu

7. **Central Bureau of Investigation (CBI) -** The website of the investigating agency was hacked, which is supposed to one of the most secure websites. The hackers mocked the country's cyber security by displaying messages.

   Impact: Website defacement.

   Source: The Times of India

8. **Indian embassy websites in 7 countries were compromised –** websites in 7 different countries were hacked to show how insecure the websites were.

   Impact: Personals details of Indian citizens living abroad were leaked by carrying out SQL injection of malicious code into the database.

   Source: The Hacker News

9. **Aadhar website**: The website was accessed and records were stolen for financial benefit.

   Impact: Data breach.

   Source: The Hindu

10. **Indian Registry for Internet Names and Numbers (IRINN)** - some business organisations dealing with enterprise security solutions bring to light a possibility of a major breach in the IRINN system leading to exposure of critical data owned by many organisations, probably around 6000 of India's ISPs were affected.

    Claim Source: SEQRITE

The IRINN system in response to the alleged breach, denied that there was any sort of major breach because of strong protocols employed, but they went on to say that they did encounter a penetration attempt externally but the attacker did not get around any important data except for some basic user profile details.

Response Source: The Economic Times

Private Sectors

1. **Zomato** - 17Million user's data stolen and put on the dark net for sale.

   Impact: Data breach.

   Source: The Times of India

2. **Reliance JIO** – The Company's servers were illegally accessed.

   Impact: Data breach by unauthorised access.

   Source: NDTV

3. **Air Indigo** – Twitter handle was hijacked.

   Impact: Not disclosed

   Source: BGR

4. **Electra card** – Fraudsters stole $45Million from ATM's worldwide.

   Impact: Data breach, $45Million stolen.

   Source: The Times of India

5. **Enstage** – Fraudsters stole $45Million from ATM's worldwide.

   Impact - Data breach, $45Million stolen.

   Source: The Hindu

6. ATM debit card breach of SBI, Axis, Yes, ICICI banks etc. –

3.2 Million Indian debit card details stolen.

Impact: Data breach, 3.2 Million debit card details stolen.

Source: The Hacker News

As noted above many websites involve database vulnerabilities that lead to loss of crucial data, it's necessary to have a well-established security plan to combat the threats that may be external or internal.

MITIGATION

- **Need for a Well Defined Security Strategy** - very important to have a strong security plan effectively imposed.
- **Eliminate the OWASP Top 10** - consists of a list of vulnerabilities every organisation must take care of in order to avoid uninvited risks, TOP10 RISKS.
- **Vulnerability Assessment & Patching** – Weekly Vulnerability Assessment & **Patch management** – This will help minimize the window of exposure.
- **Security Awareness and training** - to provide the essential education to the employees and the users about the security posture, so that they stay fool-proof.

- **Data encryption mechanisms and key exchange techniques** - to make data unusable and unreadable by intruders.
- **Review and update security policies and standards** - to know whether the organisation is abiding by the measures taken to protect itself and everything belonging to it.
- **Deception technologies -** implementation of which will help organisations to understand the behaviour of the adversary in order to amplify the security stance adopted.
- **Account Management** - to rotate, audit and control access to private assets.
- **Access Enforcement -** to prevent users from escalating their access permissions to crucial information and stored keys.
- **Least Privilege -** to limit access to the employees but provide access and resources enough to carry out their tasks with no hindrance.
- **Auditing and Monitoring** - to keep a track on who and what accessed the system, with time specifications.
- **Risk Assessment -** to discover and validate risks and threats occurring in the perimeter of the organisation.
- **Identity and Authentication** - to associate with individual users or systems and detect unauthorized access.