Aadhaar Data Leak

March 2018

* 1. billion records of Indian citizens were exposed to the internet

The breach took place on a database known as Aadhaar, the Indian government’s identity and biometric database. 89% of all Indian citizens have their information stored in this database. The data breach took place when a state-owned utility company allowed anyone to download private information on all Aadhaar holders, exposing their names, their unique 12-digit identity numbers, and information about services they are connected to.

The type of data breach was stolen information and the government was not a victim of cyber-attacks. It was only after the data was made available to the public was data stolen and anyone with a computer and very little computer skills could have downloaded the data.

The immediate threat was the personal information of all Indian citizens was accessible including name, address, phone numbers, email addresses, biometric data, consumer number, banking information, and services they were part of. Indian authorities did nothing for weeks to fix the flaw, so they found out the potential threats. Stolen information was being sold on WhatsUp for as low as $8. Their initial resolution was to pull the affected endpoint offline.

There is an endless list of policies that could have been implemented that could have prevented the data breach. The first thing they could have done was to implement app security policies to secure the API, Pentest policies may have discovered the data, vulnerability scanning policies, and authorization policies such as least privileges.

Had the government agency practiced industry standards for security, created and adhered to security policies the breach may never happened. The government agency in charge of the database denied the breach happened and even went to the extremes of trying to prosecute a reporter for breaking the news after it was discovered citizen information was available for purchase.

Authentication – Is part of “User identity and access management solutions” in DiD where a user is required to enter a private username and password to verify their identity and then as an additional layer of security multi-factor authentication, single sign-on, or lifecycle management can be used to increase security.

Authorization – Method of determining whether a user should have access to sensitive data. It is most often paired with authentication and is part of access control which is under physical security in the DiD.

Accounting – It logs sessions statistics and usage information and is used for authorization control, trends, and resource utilization. It could be used in threat assessment by analyzing potential risky habits or practices by users.

Defense in depth – By practicing Defense in Depth and implementing multiple layers of security, the potential for attack is decreased. Actively following and enforcing policies as well as being proactive in testing instead of reactive.