A 09:2021 - Security Logging & Monitoring Failures

A 09:2021: SLMF

This category is to help detect, escalate and respond to active breaches

Attack Scenario

A major Indian airline had a data breach involving more than ten years' worth of personal data of millions of passengers, including passport and credit card data. The data breach occurred at a third-party cloud hosting provider, who notified the airline of the breach after some time.

Air India reports massive data breach, personal data including passport info of 4.5 mn passengers compromised

PTI • Last Updated: May 21, 2021, 10:49 PM IST

Synopsis
Personal data -- including name, date of birth, contact information, passport information, ticket information and credit card data -- which was registered between August 11, 2011, and February 3, 2021, has been leaked of a certain number of Air India's passengers, the statement issued by the airline said.

Air India's passenger service system provider SITA faced a sophisticated cyberattack in February leading to leak of personal data of certain number of the national carrier's flyers, an official statement said on Friday.

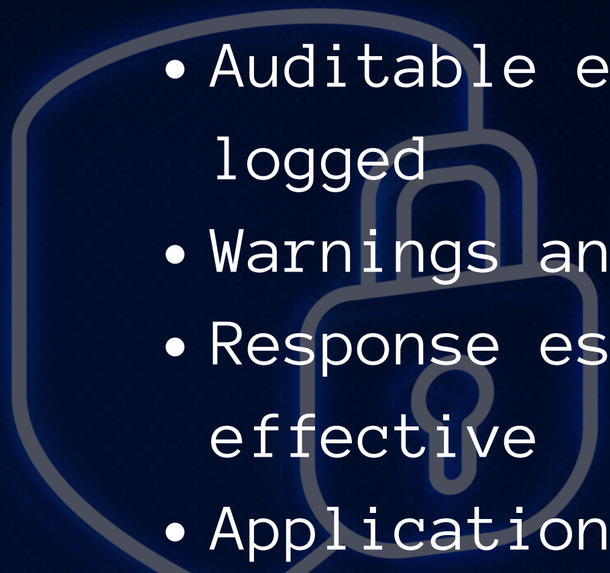
Popular in Transportation

1. Bengaluru-bound IndiGo plane declares emergency at Delhi airport

2. Passenger injured due to turbulence in SpiceJet flight dead, says airline

3. Airbus India IT pool to be biggest globally

Insufficient Monitoring



- Auditable events like logins and transactions are not logged
- Warnings and errors generate no or unclear log messages
- Response escalation processes are not in place or effective
- Application cannot detect, escalate or alert for active attacks in real-time

BUSINESS NEWS

Target Settles 2013 Hacked Customer Data Breach For $18.5 Million

The most customers ever hacked has ended in Target paying the biggest ever data breach settlement.