CASE STUDY

Briskinfosec secured Largest Commercial Bank Application

INDUSTRY
Financial Services

STANDARDS
PCI-DSS

PRIMARY SECTOR
Commercial Bank

LOCATION
East Asia

OFFERED SERVICE
Internal and External Auditing

TYPE OF SERVICES : **PCI-DSS Cyber Security Auditing**

ABOUT CUSTOMER

Our Stakeholder is one of the leading Commercial Bank throughout the globe. Our Stakeholder is offering financial solutions through its regional branches, internet and mobile. They are one of the leading banks in India who seek for setting out new standards in customer experience. They offer basic services in India like Savings Accounts, NRI Accounts, Fixed Deposits, Home Loans, Personal Loans. They have more than 15000+ employees in the organisation.

ASSESSMENT SCOPE

The Ultimate goal is to meet the PCI-DSS requirements. For accomplishing that, The Client wanted us to conduct proactive cybersecurity audits by reviewing the document and procedures for their Banking system. So we went to the organization and collected all the reports based on a various architecture such as business architecture, server architecture and infrastructure architecture. We also checked the kind of policies and procedures like password strengthening and privileges during access. The PCI DSS security requirements apply to all the system components included and connected to the cardholder data environment. The cardholder data environment (CDE) is comprised of people, processes, and technologies that store, process, or transmit cardholder data or sensitive authentication data

THE SOLUTION

By using BriskInfosec PCI-DSS standards, the consultants will have the assurance that they've PCI requirements.

Key highlights of the PCI-DSS Security are as below :

- Identifying all payment channels and methods for accepting CardHolder Data, from the point where the CardHolder Data is received through to the point of destruction, disposal or transfer.

- Documenting all CHD flows, identifying the people, processes, and technologies involved in storing, processing, and transmitting of CHD.

- Implementing controls to limit connectivity between Card Holder environment and other in-scope systems.

- Ensuring that the people, processes and technologies included in scope are accurately identified when changes are made in the organization.

- Reviewing all processes (both business and technical), system components, and personnel with the ability to interact with the Card Holder Environment.

- Collecting the existing reports of the organization, checking those and then recommending Remediations.

TECHNICAL SECURITY ASSESSMENT REPORT

At the end of the security assessment, we have identified 35 potential security vulnerabilities and then documented technical security assessment report with proper POC, and also we shared the same over protected PDF.

ISSUE TRACKING SHEET

All the identified issues were captured and will be subjected for the retest review in an XLS format.

REASSESSMENT REPORT

Overview of the entire engagement we have conducted retest on fixed issues and captured open issues which exist on the application.

CHALLENGES

PCI DSS changes in Version 3.2 (latest) of the data that are requiring increased network security are enforced in 2018.

- There are many severe vulnerabilities in SSL and early TLS that, left unnoticed, which makes organisations at risk of being breached.
- The widespread POODLE and BEAST exploits are a couple of examples were attackers take advantage of weaknesses in SSL and early TLS to compromise organisation's data.
- There are no fixes or patches that can adequately repair SSL or early TLS (TLS1.0). Therefore, it is highly essential that organisations need to upgrade to a secure alternative as soon as possible, and disable any fallback to both SSL and early TLS (TLS1.0)

THE DELIVERABLE

The reports and remediation information of the security flaws provided were customized to match the Client's operational environment and development framework. The following reports were submitted to the customer.

Key highlights of the bug fix are as below :

DAILY STATUS REPORT

All identified security issues are notified as XLS report on daily basis. Our prospect looked at the given valid report (XLS) and started working the fix right from Day 1 as they need not work laboriously on the last day when the entire report is given by the security team thus making their final assessment report easier for preparation.

By conducting an in-depth analysis of PCI requirements, Brisk Infosec alleviated the Client's risk exposure where Banking Regulatory Bodies are taking an extremely strict approach to security.

RISK BENEFITS

Brisk Infosec diminished security risks by assessing the customer's infrastructure vulnerabilities and recommended solutions with proven methods to enhance security.

COST SAVINGS

Brisk Infosec suggested cost-effective measures based on the customer's business requirements that would ensure security and continuity of the business.

CUSTOMER SATISFACTION

Security Assessments were conducted with minimum interruption and damage across customer systems to identify security vulnerabilities, impacts, and potential risks.

SUPPORT

We provide 1year support with periodic security assessment.

CONCLUSION

We educated our Stakeholder about the need to protect cardholder's data from both internal and external threats by strengthening their security. As part of the remediation stage, we recommended that their PCI compliance is being followed regularly to meet the requirements without flaws. We also worked closely with our Stakeholder to improve policies, procedures, and employee awareness programmes to increase their security maturity.

BRISKINFOSEC
TECHNOLOGY AND CONSULTING PVT LTD

+91-8608634123
044 - 43524537

contact@briskinfosec.com
www.briskinfosec.com