Briskinfosec secured The Thick Client Application for a

Largest Telecom Organization in the APAC Region

INDUSTRY

TeleCommunication

STANDARDS

OWASP, PTES, SANS, NIST, WASC, OSSTMM, NCDRC MAST

PRIMARY SECTOR

Telecommunication
Internet Service Providers
Digital Television

LOCATION

APAC

OFFERED SERVICE

Penetration Test
Security Assessment

TYPE OF SERVICES : **Thick Client Application Security Assessment**
(for a Leading Internet Service Provider)

ABOUT CUSTOMER

Our customer is one of the leading Telecommunication Organization in APAC providing high-speed fiber internet services to more than 2 million house hold customers and commercial users. They offer broadband on optic fiber with internet speeds up to 1Gbps. They are currently the 3rd largest ISP in the wired broadband category, and the largest non-telco ISP in the country.

ASSESSMENT SCOPE

Our customer has provided us with access to the thick client application through a VPN for conducting the security assessment because the thick client application is an internal application with only internal user access. Since internal users use the application , security assessment is limited to certain extent with least user privileges given to the testing team. The thick client application provided was a financial application that is majorly used to carry out transactions between the customers and our Stakeholder. This thick client application wasn' tested for past three years. Hence we had to carry out security assessment of the use in more intense manner.

PROCESSES ASSOCIATED WITH THICK CLIENT

Since our Stakeholder is a reputed Internet service provider (ISP), a financial application was used by them to monitor the internet bill transactions about how much data has been consumed by the customers. If the data pack gets exhausted, then replenishment of another internet pack was also facilitated by our Stakeholders to customers without much procrastination by instantly suggesting new schemes. All these processes are intensely associated with Thick client Software, thus making Thick client software substantially a core component for the execution of other mandatory processes.

THE SOLUTION

Briskinfosec followed Open Web Application Security Project (OWASP) TOP 10 to identify all exposed vulnerabilities in Thick client Application. Briskinfosec consultants mapped all issues with OWASP Top 10 Application Security Verification Standard (ASVS) and recommended perfect fix for identified vulnerabilities.

Key highlights of the Vulnerability fix are as below :

| Serious issues related to Input validation and authorization, session management and cookies handling were identified. The identified vulnerabilities were fixed by the Development Team.

| Platform level vulnerabilities were identified in the thick client application safeguarding the backend data of the application.

| We identified a way to reverse engineer the thick client configuration in system level and to alert Stakeholder about how unauthorised users can take advantage of this critical vulnerability.

| We completely secured the thick client application from OWASP common attack by hardening the default configuration.

| We performed vulnerability assessment by both automation and manual method for identifying the issues.

| We provided the complete Vulnerability fixing document as a reference to your development team.

THE DELIVERABLE

The reports and remediation information provided were customized to match the stakeholder operational environment and development framework. Identified security issues were categorized through code fix, configuration fix and best practices to make stakeholders understand the criticality of each vulnerabilities. The following reports were submitted to the customer.

DAILY STATUS REPORT

This thick client security assessment consumed around 1-2 weeks of time including retest. During the process of thick client testing, issues were identified and we shared all identified issues with corresponding recommended FIX over mail on a 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.

TECHNICAL SECURITY ASSESSMENT REPORT

Complete security testing was carried. All the detected issues and the proof of concept (POC) will be covered with detailed steps in a PDF format.

ISSUE TRACKING SHEET

| All the identified issues were captured and will the be subjected for the retest review in a XLS fomat.

| All the issues will be captured for the reassessment.

SECURITY ASSESSMENT REPORT

Step by step process carried out by the entire team for each vulnerability.

OWASP ASVS MAPPING SHEET

Application Security Verification Standard Checklist was updated and shared the same.

FINAL BUG FIX REPORT

Overview of the entire engagement, the issues that were identified, the recommendations and remediation which were made to mitigate the threats.

THE CHALLENGES DURING ASSESSMENT

Since the application is a thick client, we faced difficulties in testing certain areas of application like Proxy configuration, backend database, and network traffic etc. Briskinfosec used complex application testing procedure by synthesizing the usage of both automated and manual security tools to identify some critical vulnerabilities in application after bypassing certain built-in security controls of the thick client app.

STAKEHOLDER BENEFITS

RISK BENEFITS

Briskinfosec alleviated the security risks by assessing the customer's infrastructure vulnerabilities and recommended solutions with proven methods to enhance security.

COST SAVINGS

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

BRIEFINGS

We have advised on many cybersecurity crisis management and incident response matters, ranging from inside jobs and social engineering to sophisticated criminal hackers penetrating our clients' systems. Due to the sensitive nature of cyber breaches, we have created a perfect case study to demonstrate the incident response considerations and remedial actions an organization could experience. The case study is inspired by real matters upon which we have advised based not only on individual consideration but universal consideration.

CUSTOMER SATISFACTION

Mobile Application Security Assessment was conducted with minimum interruption and damage across customer systems to identify security vulnerabilities, impacts, and potential risks.

SUPPORT

We have offered one year support with periodic security assessment to maintain mobile app security on highest standard.

CONCLUSION

We advised our Stakeholder on the measures that should be taken to remedy the various deficiencies in their systems and processes. As part of the remediation stage, we recommended that their day to day network should be segregated from the network that stores sensitive personal information and financial systems. We worked deeply with our stakeholder and also educated about the indispensability to improve the policies, procedures, and employee awareness programmes to increase their cyber maturity.

BRISKINFOSEC

TECHNOLOGY AND CONSULTING PVT LTD