CASE STUDY

Briskinfosec secured Infrastructure Of Reputed Insurance Provider

INDUSTRY
Financial Services

STANDARDS
OWASP, OSSTMM,PTES, WASC, SANS, PCI DSS, ISO27001, NIST SP800-115

PRIMARY SECTOR
Banking Company

LOCATION
India

OFFERED SERVICE
Host Level Security Assessment

TYPE OF SERVICES : **Securing Infrastructure Of Reputed Insurance Provider**

ABOUT CUSTOMER

Our Stakeholder is one of the largest employing organization spread across their banking, technology and shared services operations. Our Stakeholder has been a top 5 arranger of domestic debt since 2010 and a top 3 arranger of offshore bonds in 2012. Their commitment to growing franchise is best demonstrated through their investment of more than $800million of capital in India, among the largest capital commitments by any foreign bank. Wealth & Investment Management, which operates through Stakeholder's Securities & Investments Pvt Ltd (BSIPL), have attained a leading position within just five years of being set up and has also been voted as the Best Private Bank in India by "The Asset" for three years in a row. They are also one of the leading private general Insurance Company having 759 branches

ASSESSMENT SCOPE

Our client wanted us to perform Host Level Security for Windows 7/Xp and for applications like SQL, Apache, IIS Servers as well as routers and switches to identify potential and actual weaknesses, thus recommending specific countermeasures in their infrastructure. A host security assessment is performed from the point of a host to evaluate the security of the company's critical servers. So, we analyzed the operating system and Host-level security issues in the operating environments.

THE SOLUTION

By using BriskInfosec frameworks, the Security team of Briskinfosec completed the Host Level Security bug fix and recommended best practices using the Penetration Testing Execution Standard (PTES)

Key highlights of the bug fix are as below :

- We encountered some serious issues related to SSL attacks, Weak encryptions, Captured NTLM Hashes to crack passwords, SMB login default credentials issues were identified and fixed by the Network Team.
- Security-related patches for the operating system was not deployed properly.
- We came across presence of Trojans and backdoor.
- Unnecessary protocols were enabled.
- Host-Level firewall rules were weak, and we found some suspicious file existence.
- Account Management related issues.
- We performed Host security by both automation and manual method in identifying the issues
- We provided the complete bug fixing document with best practices as a reference to your Network Team.

THE DELIVERABLE

The reports and remediation information provided were customized to match the Client's operational environment. The following reports were submitted to the customer: Key highlights of the bug fix are as below :

DAILY STATUS REPORT

This Host level security assessment consumed around 1-2 weeks of time including retest. During the process of assessment, issues were identified and we shared all identified issues with corresponding recommendation 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

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 the be subjected for the retest review in an XLS format.

FINAL BUG FIX REPORT

Overview of the entire engagement, the issues identified and the recommendations made to mitigate the same.

CHALLENGES

Those challenges are :

- Sometimes while accessing the requirements, there would be restrictions even after which the customers demand that particular information.
- If a particular server is too strictly configured, then nothing lucrative can be done.

However, with sheer grit and perseverance, Briskinfosec successfully alleviated the Stakeholder's risk, where the Banking bodies are taking an extremely strict approach towards security.

RISK BENEFITS

BriskInfosec diminished 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.

SUPPORT

We provide 1year support with periodic security assessment.

CUSTOMER SATISFACTION

Host Level Security Penetration testing was conducted with minimum interruption and damage across customer systems to identify security vulnerabilities, impacts, and potential risks.

CONCLUSION

We advised the Stakeholder on the measures they should take for rectifying the various vulnerabilities in their Host systems. For remediation, we also educated them about the various mandatory processes such as completely monitoring of their Host systems on a monthly basis and log monitoring also to be done consistently. We also worked closely with our Stakeholder for improving policies, procedures and employee awareness programmes for increasing security maturity.

BRISK INFOSEC

CYBER TRUST & ASSURANCE

BRISKINFOSEC

TECHNOLOGY AND CONSULTING PVT LTD

+91-8608634123
044 - 43524537

contact@briskinfosec.com
www.briskinfosec.com