ENSURING SECURITY OF CLOUD-BASED PLATFORM

The Client's Profile

The client is a leading HR Consulting Firm in India. They provide HR Outsourcing Services like Payroll Execution and Employee Lifecycle Management solutions using the Software-as-a-Service (SaaS) platform. In 2002, our client led the way for e-filling income tax returns for the Department of Income Tax in India. The company set the benchmark for outsourcing HR solutions and become the first provider offering online, semi-online and offline services to corporate and salaried individuals for their income tax and finance-related solutions.

Challenges Faced by the Client

Our client, one of the reputed IT service-providing companies did great work at simplifying critical operations for its clients by offering solutions based on cloud computing. However, the firm was constantly plagued by the idea of security attacks that most online clouds are vulnerable to. The attacks may include Internet malice like:

- Session Hijacking
- Denial of Service
- Injection
- Data Loss through Malware
- Buffer Overflow

To protect their cloud from such threats seemed like a daunting task and they were constantly striving towards formulating a robust strategy that could prevent against them.

Client's Key Security Concerns

- Bringing prevailing IT practices in sync with best practices followed globally
- Detecting issues even before they come to the attention of other people
- Bringing ease and discipline when implementing information security measures

The Security Solution Provided By Flatworld

Flatworld provided an effective solution to safeguard the cloud by means of an Information Security Program and implementing the best practices in information security. The first step of the process was to identify the points where the system was most vulnerable: this was done based on the OWASP Top 10 criteria by means of penetration tests. Following the tracking of vulnerabilities, our software team resolved the concerns and then repeated tests to check for remaining or any newly emerged issues.

After consulting with the management at customer's end, we built a Calendar of Activities. We assigned Information Security Officers (ISO) who efficiently liaised with the customer to implement best practices of information security in coherence with global standards as well as the IT security policies of the end clients our customer serviced.

Steps We Followed

- Discussed concerns with the management
- Assessed the prevailing IT Security Policy of the company to identify the cause of the problems being faced by the company
- Chalked out a Calendar of Activities in coordination with the management
- Implemented the best practices in security
- Improved the control environment by executing best practices followed by the industry
- Listed potential assets for the purpose of security testing
- Tested vulnerabilities to remove all inaccuracies and false positives from the system
- Executed advanced testing techniques which worked efficiently against all verified vulnerabilities
- Discussed findings of vulnerabilities and threat assessment and suggested corrective actions to customers

Benefits Rendered

- Enhanced security
- Ensured compliance of legal, regulatory, contractual and statutory requirements
- Executed structured way to maintain information security, resulting in reduction of efforts
- Protection of confidential and business critical information
- Prepared the client for internal and external audits

If you'd like to hire our experienced software professionals, or want to outsource software development services to us, please feel free to get in touch with our expert team.