ENTERSOFT

SECURITY IN FINTECH

Security forms the foundation of the financial services industry

Why security in FinTech?

One side is the cautious, steady moving world of banks and financial institutions while the other is the dynamic, entrepreneurial environment of software and technology companies which are moving into the fintech space.

Aside from convenience, keeping customer information secure is the biggest responsibility of all fintech companies.

1 ABOUT

The Australia-based client develops applications and software for banks to make their internal processes easier and faster.

We were approached to help secure an application that analyses and integrates bank statements; and makes them retrievable instantaneously.

2 THE CHALLENGE

Client was in talks with the largest bank in Australia to get their application implemented for the bank's processes.

The bank adheres to extremely strict standards when it comes to security and compliance.

Client was asked to obtain ISO 27001 certification and strengthen their framework of policies and procedures involved in security management processes.

The framework, once updated was to be thoroughly examined by the bank before the application was deployed.

3 QUICK OVERVIEW

16

policies revised and implemented

14

processes made smoother and safer

15

vulnerabilities found after two consecutive penetration tests

50,000

lines of documentation analysed and improvised

ISO 27001

ready in 45 days. Tests completed in 15.

4 METHODOLOGY

We follow a complex and systematic approach that addresses all elements of cybersecurity, which helps organisations be better equipped and educated to battle the full spectrum of future attacks.

SECURITY CULTURE ADOPTION

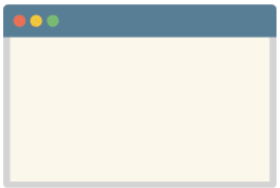
Implementation of a comprehensive information security policy.

A formal review to identify vulnerabilities and assess risks, with tests conducted once a year and whenever the environment changes.

APPLICATION SECURITY TESTING

Year long real time cyber attacks to strengthen the apps. The following are performed proactively on a regular basis:

- MAST/WAST
- API Security Tests
- Cloud Security Tests
- Code Reviews



POLICY & PROCESS

Creation and development of security processes and policies. Build secure code with best practices in data security.

Information security practices that comply with or exceed latest standards.

COMPLIANCE

Network components, processes, and custom software are tested on a regular basis to ensure that cybersecurity measures are still effective, especially after deploying new software or making changes to the system's configuration. Through network of compliance partners, we provide required assistance to obtain the compliance/certification.

5 POLICIES & PROCESSES

POLICIES FRAMED

- Anti-virus Policy
- Backup Policy
- Email Policy
- Firewall Policy
- Infra Details
- Internet Usage Policy
- ISMS Do's and Don'ts
- Laptop Policy
- Password Policy
- PDA Policy
- Router Policy
- Server Policy
- Server Security Policy
- Software Usage Policy
- VPN Policy
- Privacy Policy

PROCESSES IMPLEMENTED

- Access Control Process
- Business Continuity Process
- Change Management Process
- Client Management Process
- Communication Operative Information Process
- Compliance Control Process
- Environmental Provision Process
- Incident Management Process
- IT Asset Management
- Patch Management Process
- Physical Environmental Process
- Risk Management Process
- Secure Coding Process
- Service Levels and Support

6 EXCLUSIVE TESTS

"Program testing can be used to show the presence of bugs,
but never to show their absence."
- Dijkstra (1970)

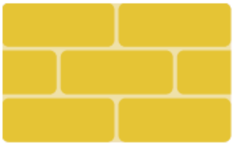
At times we operate outside our normal course of action to identify vulnerabilities that may not be visible after performing the usual tests.

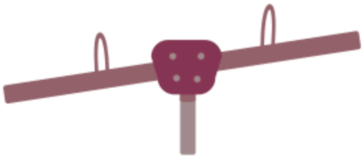
DDoS Attack

We launched a real time, small scale DDoS attack to check the resilience of the existing DDoS evasive configurations.

Web Application Firewall Testing

Client had configured a third party web application firewall which needed to be thoroughly tested for external stress.





Reviewing the load balancer

Hand in hand with DDoS tests , load tests were performed to validate the cloud configurations.

Cloud infrastructure assessment

OSSTMM and AWS cloud best practices were tested to ensure that compliance needs were met.

BANGALORE

+91 80 4150 1408
info@entersoftsecurity.com
www.entersoftsecurity.com

BRISBANE

+61 7 3376 9381
info@entersoft.com.au
www.entersoft.com.au

SINGAPORE

+65 6519 0757
info@entersoftsecurity.com
www.entersoftsecurity.com