CASE STUDY

RISK-DRIVEN APPLICATION TESTING SERVICE

OVERVIEW

Industry: Financial

A large financial organisation, who provides online transaction services in over 30 countries, identified over 500 business-critical web applications that had launched without secure controls implemented in either their design or development.

Since the applications were not based upon 'security by design' principles or subject to fundamental and standardised secure coding best practices, a risk baseline was not established on which to determine hosting controls or conduct routine security penetration testing with any assurance.

Consequently, each application was subject to a common security penetration test approach in which it was assessed only against generic publicly-recognised security vulnerabilities. Application-specific design and development weaknesses were unidentified and therefore unaddressed in testing.

Remedial measures identified in this standardised testing approach were implemented by the client but did not reduce the number of breaches they were experiencing.

In short, the significant budget spent on application security penetration testing by this client did not reduce risk and had no real return on investment.

THE CHALLENGE

Deliver a cost-effective application security testing methodology to both identify and address security vulnerabilities specifically associated with each individual application as a result of security controls not implemented in its design and development stage.

INHERENT FLAWS

To mitigate the inherent design and development flaws, each was required to produce application-specific remedial measures.

SERVICE INTERRUPTION

As the applications were already live, all testing had to be conducted without service interruption to ensure a smooth customer experience.

TIME TABLE

Schedules had to be maximised to adhere with the quick turn-around time needed as since the application was live and vulnerable to attacks.

THE SOLUTION

To meet this daunting requirement, Risk Crew implemented its Risk-Driven Application Security Testing Service for the client.

This innovative service is founded on the principle of 'security by design' and is comprised of the following step-by-step activities for each application:

THE RESULTS

By implementing a more holistic 'risk driven' security penetration methodology the client significantly enhanced the security integrity of the business critical web applications, **reducing the risk of a breach** and obtaining a substantially bigger return on the security testing programme spend.

By documenting the individual risks and attack surfaces associated with the applications, the client received critical information for **enhancing and ensuring the security configuration and change management procedures** required to support the application throughout its use.

The service resulted in both **risk reduction and cost-savings**. It doesn't get better than that.

THE PROVEN 4-STEP PROCESS

STEP 1 DESIGN REVIEW

Risk Crew conducted a detailed review of the design, development, testing and hosting documentation associated with the application. The objective was to identify all of the application's access points, existing access controls and security vulnerabilities associated with the design. Also, sample code reviews were conducted.

A detailed report was produced with the findings and recommendations for addressing vulnerabilities in the design and future development stages.

STEP 2 THREAT & ATTACK MODELING

The design review was followed by a Risk Crew conducting an application security threat and risk assessment for the application. In this step, the information assets processed, stored, or transmitted by the application and their sensitivity classification levels were identified and confirmed with the client.

An information threat and risk assessment was then conducted for the application based upon the information obtained in the design review identifying the risk associated with poor design and development practices. Results were added to the client's risk register for inclusion in their risk management procedures.

STEP 3 THREAT ASSESSMENT

The results of the threat assessment provided valuable data for the next step of defining and documenting the 'attack surface' associated with the application given its design, development, and deployment flaws.

This work was critical and done to identify the probable threat agents and their most likely attack vectors. This modeling was essential for scoping customised (and therefore effective) security penetration testing for the application that actually simulated real-life attack scenarios.

Upon completion, the model to the client for record to be used as a baseline testing scope for the application.

STEP 4 SECURITY PENETRATION TESTING

Finally, Risk Crew conducted security penetration testing for each application based upon the information obtained in the first 3 steps.

The testing scope, approach, tools & methodology were determined by the actual attack surfaces associated with each application.

In this way, the penetration testing simulated real-world attack scenarios, from threat agents through attack vectors specifically associated with each application given its inherent design and development vulnerabilities. The simple logic of testing the actual attack surface associated with the application reaps enormous rewards.

risk crew
+44 (0) 20 3653 1234
riskcrew.com
5 Maltings Place
169 Tower Bridge Road
London, SE1 3JB
United Kingdom