IT Security Professionals

FMA
Risk Management Solutions

Services Datasheet

Application Vulnerability Assessment

OBJECTIVE

- Create a snapshot of your current security posture.
- Identify all security bugs in your applications.
- Identify patterns of flaws to discover flaws based on vulnerabilities already discovered to save time and be more complete.
- Document findings in a comprehensive report.

BENEFITS

- We find holes in your web applications, SOA servers, Web Services servers, RMI and CORBA servers.
- We do manual testing for accuracy and effectiveness.
- We offer to our customers active knowledge transfer of techniques, issues and remediation.
- We address your regulatory security requirements.
- We improve your security awareness in technical and non-technical staff

DELIVERABLES

- AppVA Executive Summary.
- AppVA Technical Report, containing for each flaw the detailed reasons, consequences and remediation.
- Technical support on the remediation techniques.
  (All reports can be written either in English or in French).

RELATED FMA SERVICES

- Network Penetration Test.
- Source Code Security Assessment.
- Operating System Vulnerability Assessment.
- Writing Secure Code (Java, C/C++, ASP, PHP).

One of the most significant source of vulnerabilities that many companies fail to address, or even recognise, is their applications. The best security defences can be rendered essentially useless if an organisation is using an insecure application. The significance of this security risk grows daily as more and more organisations rely on mission-critical applications for their core business. Application Vulnerability Assessments (AppVA) are aimed at identifying and minimising the risk that applications introduce vulnerabilities within the core environment.

FMA conducts professional Application Vulnerability Assessments against applications within your LAN, WAN, Intranet and Internet sites in order to expose applicative holes. An Application Vulnerability Assessment could be called an Application Penetration Test if you will, it is a simulation of a real-world outside attack against an application in order to identify security weaknesses before they are exploited by hackers.

Although applications may be encroached during the Application Vulnerability Assessment, FMA will never attempt to erase, alter or harm any of your company's data. This test is done with absolute safety of your application and infrastructure in mind. Engagements typically range from a few days to three weeks.

Why FMA Professional Services?

- Exclusively focused on IT security services.
- Advanced Methodology compliant with best security testing practices defined in OSSTMM, OWASP and IBTRM guides.
- FMA is more than 6 years old and has an extensive track record.
- Jargon-free detailed findings and recommendations.
- Reasonable ongoing technical support at no additional cost.
- We can perform testing on-site or remote and can work 24/7.
- We can test within given change control windows and during quiet periods.

Premier IT Security Professionals

When recruiting consultants, FMA's first priority is security expertise. Members of ours team are passionate about security and have diverse IT security backgrounds. All our consultants are premier professionals with extensive IT security experience (more than 8 years) and are among the most technically proficient in the industry. Additionally, most of them are regular speakers at international IT security conferences.

Methodology

A large part of FMA effectiveness comes from having developed a thorough technical methodology that is reliable, repeatable and that definitely goes well beyond automated tools.

http://www.fma-rms.com/
info@fma-rms.com

IT Security Professionals

FMA Risk Management Solutions

Methodology

Application Vulnerability Assessment

FMA Risk Management Solutions
10 Anson Road,
#15-14 International Plaza,
Singapore 079903,
Republic of Singapore
Tel: (+65) 92997327
Fax: (+65) 67220785

Additionally to operating in Singapore, we often provide IT security services to organisations located in Indonesia, Malaysia, Hong Kong, Thailand and China.

We perform Application Vulnerability Assessment engagements either on a one-time basis, or on a subscription basis (e.g. re-test application after updates are applied or a new version is released).

Thorough Manual Testing

Because of the significant limitations of automated testing tools like application vulnerability scanners, almost all of our testing is performed and verified manually using a well-defined, repeatable and consistent methodology.

Automated tools are used in areas of the assessment only where they are proven to be accurate and effective (less than 5 percent of a typical engagement).

The test cover in depth the four areas of application security: confidential information disclosure, application input manipulation, session related issues and logic flaws.

Footprinting: gathering information on the application independently of what is provided for the assessment.

Scanning: inventory of functionalities on the application. This allows the penetration team to focus on the best avenues of entry.

Enumeration: performing more intrusive probes. May involve performing CGI script parameters fuzzing, sending malicious inputs in order to coerce the application to reveal information.

Gain access: using information gathered from previous stages, vulnerabilities are exploited (no harm approach).

Escalate privileges: attempting to gain full control of information assets on the application by obtaining administrative access to the application, or by performing logic flaws etc...

Harvest: collecting sensitive and valuable information that can be stolen.

Reporting: a comprehensive report, listing vulnerabilities and recommended countermeasures is prepared. In addition, a database with functionality targeted, vulnerabilities detected, risk level, access gained, etc. is provided for the administrators to action.