

application security assurance

[commissum - that which is entrusted]

commissum is able to provide a comprehensive range of application security assurance services that encompass design assurance consultancy throughout the development lifecycle, development audit, critical phase review, and specialist security application testing

issues

The ability to run applications is a main driver for using complex computer systems. They are the means of harnessing the power of the hardware to provide value through functionality; the access points to your information assets.

Unfortunately applications are frequently the weak points in system security. In today's environment, time-to-market is critical for application development. There is always a delicate balance between functional requirements, business needs, and security risk.

Organisations are understandably focused on ensuring that business functional requirements are delivered by developers. In this environment, it is too easy to overlook critical flaws in design or underlying vulnerabilities in the commercial-off-the-shelf components that are inevitably part of the application, or part of the environment in which it operates.

Attackers are only too aware of this potential weak link, and application level attacks are increasingly the source of unauthorised access to or misuse of systems. By their nature, they often bypass traditional defences, and are extremely difficult to detect.

Ideally, a client will engage the services of **commissum's** assurance specialists at the earliest phases of a project; it is significantly more cost effective to design with best practice security in mind from the start. However, the knowledge and skills of the **commissum** team can be applied at all stages; particularly as independent security testers as part of system proving.

approach

commissum's application security assurance services encompass design assurance consultancy throughout the development lifecycle, development audit, critical phase review, and specialist security application testing. Depending on agreed scope, elements addressed include:

- appropriate and effective segregation and control of access
- non-essential functions exposed to users or other applications
- monitor network traffic for transmission of information of benefit to an attacker
- resilience to inappropriate data
- review & test systems software for known security flaws and a range of typical vulnerabilities
- infrastructure implementation for secure operation
- protection of sensitive information and administrative functions
- comprehensive application testing; drawing on concentrated security knowledge to devise tailored threat scenarios

It is important to remember that meeting functional and performance requirements alone are insufficient; thinking like an attacker is different from thinking like a user.

customer benefits

commissum's independent and objective advice provides clients with:

- a concentrated pool of security focused resource to advise on best practice security implementation
- objective, independent advice on the issues surrounding bespoke software development as well as current detailed knowledge on a wide range of commercial software applications
- guidance on best practice control measures and corrective action required to improve security deployment and integrity
- independent expert assurance that applications and processes are able to resist a range of attacks
- recommended hardened configurations for system components that enable required functionality while disabling unneeded features; improving integrity and resistance to attack
- confidence that their systems will not make headlines as the latest victims of poor application security

“At last I am going to be well”

Paul Scarron (1610 - 1660)
As he lay dying.