Which Security Assessment Provider?

Author: Glyn Geoghegan, Corsaire

Published: Wednesday, 13 October 2004 11:28 GMT

Having identified a requirement for Security Assessment, be it an external penetration testing, security assessment or policy audit, it is vital to find an appropriate security services partner. Whether the Security Assessment is driven by an audit requirement, due-diligence or a compelling event, it is highly likely that there will be a requirement for a third party to conduct the work.

Furthermore, the findings and advice identified as a result of the work may need to satisfy internal or external auditors, the board or shareholders.

As such, it is clearly important that the style and content of the assessment, those performing the work and the deliverables (i.e. the reports) satisfy the technical requirements set down. Perhaps more importantly, they must also reflect a business understanding within the context of the project, and be able to present and articulate this to technical and non-technical target audiences.

The Security Assessment field is rapidly becoming an industry in its own right. Business demand has grown alongside the proliferation of information regarding vulnerabilities, their exploitation and remediation.

Corporate Internet presence has developed from simple, static brochure sites to increasingly complex interactive applications allowing potential customers and partners alike to delve into the data and systems at the heart of the enterprise.

Types of Assessment

Due to the increasing complexity of IT infrastructure and services, penetration testing and security assessment are no longer simple exercises. The requirement may be for a security health check of the underlying infrastructure, comprising vulnerability identification and analysis within the publicly available shrink-wrapped devices and software.

Increasingly, the scope also needs to include a security evaluation of the bespoke elements of the environment. This could be a full proprietary web-enabled application allowing users to initiate transactions, accessing and modifying back-end data, for example Internet Banking. It may also be a small collection of scripts handling customer contact or queries, or the configuration of a document presentation and content management application.

Other bespoke technologies may be involved. For example, the site could be enabled for mobile access, wireless technology may be deployed, integrated Voice and Data systems; all presenting new security risks.

It's important to keep sight of what we are trying to achieve and protect through the assessment - generally the objective is to safeguard the core intellectual and electronic assets of the organisation, and to ensure compliance with regional and global, IT and data safeguard laws such as the UK DPA, US HIPAA, ISO17799 etc. As such, the broad types of assessment that need to be available are as follows:

External Penetration Testing is the traditional approach to security assessment. The testing is focussed on the servers, infrastructure and the underlying software comprising the target. It may be performed with no prior knowledge of the site (black box) or with full disclosure of the topology and environment (crystal box). This type of testing should typically involve a comprehensive analysis of publicly available information about the target, a network enumeration phase where target hosts are identified and analysed, and the behaviour of security devices such as screening routers and firewalls are analysed. Vulnerabilities within the target hosts should then be identified, verified and the implications assessed.

Internal Security Assessment follows a similar methodology to external testing, but provides a more complete view of the site security. Testing will typically be performed from a number of network access points, representing each logical and physical segment. For example, this may include tiers and DMZ's within the environment, the corporate network or partner company connections.

Application Security Assessment is designed to identify and assess threats to the organisation through bespoke, proprietary applications or systems. These applications may provide interactive access to potentially sensitive materials, for example. It is vital that they be assessed to ensure that, firstly, the application doesn't expose the underlying servers and software to attack, and secondly that a malicious user cannot access, modify or destroy data or services within the system. Even in a well-deployed and secured infrastructure, a weak application can expose the organisation's crown-jewels to unacceptable risk.

Wireless/Remote Access Assessment (RAS) Security Assessment addresses the security risks associated with an increasingly mobile workforce. Home-working, broadband always-on Internet access, 802.11 wireless networking and a plethora of emerging remote access technologies have greatly increased the exposure of companies by extended the traditional perimeter ever further. It is vital that the architecture, design and deployment of such solutions is secure and sound, to ensure the associated risks are managed effectively.

Telephony Security Assessment addresses security concerns relating to corporate voice technologies. This includes abuse of PBX's by outsiders to route calls at the targets expense, mailbox deployment and security, voice over IP (VoIP) integration, unauthorised modem use and associated risks.

Methodologies, Certifications and Standards

The Security Assessment industry has grown rapidly, and clients are now presented with a bewildering array of vendors offering services. Unfortunately, the development of practical and appropriate standards and accreditations has lagged behind. Because of this it is imperative to consider whether the prevailing standards are suitable or appropriate for your requirements.

Methodologies:

Compliance with formal methodologies helps ensure that an assessment is both repeatable and of a consistent standard.

CHECK The CESG IT Health Check scheme was instigated to ensure that sensitive government networks and those constituting the GSI (Government Secure Intranet) and CNI (Critical National Infrastructure) were secured and tested to a consistent high level. The methodology aims to identify known vulnerabilities in IT systems and networks which may compromise the confidentiality, integrity or availability of information held on that IT system. CHECK consultants are only required when the assessment for HMG or related parties, and meets the requirements above. In the absence of other standards, CHECK became the de-facto standard for security assessments and penetration testing in the UK. However, open source methodologies such as the following are providing viable and comprehensive alternatives, without UK Government association.

OSSTMM The aim of The Open Source Security Testing Methodology Manual is to set forth a standard for Internet security testing. It is intended to form a comprehensive baseline for testing that, if followed, ensures a thorough and comprehensive security assessment has been undertaken. This should enable a client to be certain of the level of technical assessment independently of other organisation concerns, such as the corporate profile of the penetration test provider.

OWASP The Open Web Application Security Project (OWASP) is an Open Source community project developing software tools and knowledge based documentation that helps people secure web applications and web services. OWASP is an open source reference point for system architects, developers, vendors, consumers and security professionals involved in designing, developing, deploying and testing the security of web applications and Web Services. In short, the Open Web Application Security Project aims to help everyone and anyone build more secure web applications and web services.

The key areas of relevance are the forthcoming Guide to Testing Security of Web Applications and Web Services and the testing tools under the development projects. The Guide to Building Secure Web Applications not only covers design principals, but also is a useful document for setting out criteria by which to assess vendors and test systems.

Certifications:

Organisational and individual certifications are also useful in gauging whether a supplier is qualified to satisfy the testing requirements. As although some certification schemes apply to the organisation as a whole, they are typically focussed on the individual team members.

CISSP The CISSP certification was designed to recognise mastery of an international standard for information security and understanding of a Common Body of Knowledge (CBK). This CBK covers ten domains of security knowledge covering the management, theory and implementation, and certifies holders have a broad understanding of InfoSec.

SSCP The SSCP certification recognises practitioners of information security [IS] and understanding of a Common Body of Knowledge (CBK). It focuses on practices, roles and responsibilities as defined by experts from major IS industries.

CISA The CISA certification is ISACA's cornerstone certification. Since 1978, the CISA exam has measured excellence in the area of IS auditing, control and security. CISA has grown to be globally recognized and adopted worldwide as a symbol of achievement.

CISM The CISM certification is ISACA's new certification and is specifically geared toward experienced information security professionals. CISM is business-oriented and focused on information risk management while addressing management, design and technical security issues at the conceptual level. It is for the individual who must maintain a view of the "big picture" by managing, designing, overseeing and assessing an enterprise's information security.

CLAS The CLAS certification is the CESG Listed Adviser Scheme - a partnership linking the InfoSec knowledge of CESG with the expertise and resources of the private sector. It is designed to ensure that certified consultants have a level of knowledge regarding current UK Government policy and guidance, the risks to InfoSec and the appropriate techniques to counter them.

Standards:

There are a number of standards and acts relating to general Information Security, including industry specific schemes. These include ISO17799, the UK Data Protection Act, the US Health Insurance Portability and Accountability Act (HIPAA), VISA and MasterCard schemes; together with numerous international and regional acts and legislation.

These standards are beyond the scope of this document, but it is important to determine which standards are relevant, appropriate and required. The chosen security services supplier should be familiar with them, particularly where compliance is to be assessed.

Choosing Your Security Assessment Partner

Having determined the objectives from the assessment, and the scope required, the following should be asked of a potential supplier to determine whether they are appropriate.

1. Are they security specialists first and foremost, or is the security practice a secondary concern?
2. Does the organisation's methodology follow and exceed those such as OSSTMM, CHECK and OWASP?
3. Do they offer a comprehensive suite of services, tailored to the specific requirements of their clients?
4. Are they able to distinguish and articulate between infrastructure and application testing?
5. Are their staff experienced security professionals, holiday recognised certifications such as CISSP?
6. How many technical staff work on security and assessments?
7. How many of those are dedicated solely to security?
8. Do the deliverables, such as the final report, present the results in an informed manner, with concise and practical information for technical and non-technical parties?
9. Are they recognised contributors within the security industry?
10. Are references available to attest to the quality of past work performed?

Conclusions

Third party validation of organisations'security is becoming more prevalent (and indeed required), through security assessments.

In order to ensure that testing is of the required quality and depth, clients must ensure their suppliers are able and qualified on a number of levels. This can in part be achieved by ensuring the methodologies in use are compliant with, and ideally exceed, those in the public domain.

Furthermore the credentials and experience, and therefore ability, of those involved in the project should be reviewed. This should relate both to their technical knowledge and the ability to convey that information to technical and non-technical audiences within the appropriate context.

By selecting suppliers based on these criteria, and rotating the assessment programme between a small number of trusted suppliers, organisations can demonstrate a level of due-diligence and compliance. In turn, this should greatly improve the security posture, and perception, of the organisation in the eyes of auditors, partners, investors and clients alike.