INTERHACK

Interhack
5 E Long St 9th Fl
Columbus, OH 43215

VOX +1 614 545 HACK
FAX +1 614 545 0076
WEB http://web.interhack.com/

UNDERSTANDING INFORMATION ASSURANCE SERVICES

C. MATTHEW CURTIN, CISSP

Among purchasers of security services, a great deal of confusion exists about what kinds of services are available and what can be expected of each type of service. Here, we discuss *assessment*, *evaluation*, and *penetration testing* in terms of deliverables and key benefits for achieving the high-order goal of information assurance.

There are three key differences among these three levels of service. The first is "shelf life," that is, how long the report that results will be useful. The second difference is breadth of consideration, how broadly information security will be considered. The final difference is depth, just how deeply into the technology and implementation the service will go.

Assessment provides the broadest consideration, with the greatest shelf life, but with the least depth, and is thus an appropriate starting point.

Evaluation establishes whether systems are in compliance with specific standards in a cooperative effort with the organization, narrowing the focus somewhat, with shorter shelf life, and with greater depth.

Penetration Testing determines whether a specific target is vulnerable to a specific attack at a specific point in time. This consideration is the most narrow, has the shortest shelf life of all, and the greatest technical depth.

The key to success in information assurance spending is understanding your needs and what can be done to address them given the resources available.

Introduction

The U.S. National Security Agency (NSA) has developed the Information Assurance Training and Ratings Program (IATRP) to help government organizations trying to raise their information security (INFOSEC) posture in general or specifically trying to comply with the Presidential Decision Directive (PDD)-63 requirement for Vulnerability Assessments.

NSA has identified three levels of system review. These are known as *assessment*, *evaluation*, and *penetration testing*.

To help to reduce the amount of confusion surrounding security services, Interhack supports efforts in useful standardization of terminology and metrics throughout industry and government concerns. To help potential clients understand how their needs are addressed, Interhack offers the following brief explanations of each type of service.

Level I: Assessment

Assessment is a high-level review of the organization's critical information and a qualitative consideration of the impact of various types of security incidents. It has the greatest shelf-life, providing not only immediate-term direction for remediation, but also longer-term direction about how to improve the overall information security posture of the organization.

Interhack uses NSA's INFOSEC Assessment Methodology (IAM) for performing these assessments.

IAM is made up of three major phases: pre-assessment, on-site assessment, and post-assessment. Pre-assessment involves an on-site working meeting with key members of the sponsoring organization to identify critical information types and review of critical documentation, system configuration notes, and all other relevant formal documentation. The On-site Assessment involves a series of interviews of key members of the sponsoring organization and observation of system demonstrations, in an attempt to understand informal policy and procedure. A presentation is then given to the sponsors, showing initial findings, and allowing the organization to ask questions and to express any concerns. The final phase, post-assessment, is the creation of the formal report of findings.

Key benefits of assessment is that it provides the organization with the greatest value for getting started in understanding its information security posture, seeing where its defenses should be concentrated, and how it stands up in eighteen different areas of information security consideration.

Level II: Evaluation

Evaluation is a detailed review of the organization's information systems, with specific regard to the systems' ability to enforce policy. Evaluation is cooperative in nature, and provides tasks for remediation, as well as medium-term direction on how to use technology to support information security. Evaluation teams are known as "Blue Teams" in military jargon.

NSA is presently working on its methodology for system evaluation. Until that standard is released, Interhack employs its own methodology for evaluating system security, keeping in mind best practices as defined by industry needs, ongoing research, and projects of standards bodies such as National Institute for Standards and Technology (NIST) and the Internet Engineering Task Force (IETF).

Evaluation starts with the definition of scope: which systems are to be included. This nicely fits in with Assessment, as an assessment following IAM will have identified critical systems based on informational criticality in the organization. Once target systems are defined, a standard is created from organizational policy, industry regulation, and best practice. Evaluation then begins, testing for adherence to the standard. An initial report is released to the sponsoring organization, providing it the ability to raise questions or concerns before the completion of the final report.

The final report will include INFOSEC findings, showing where policy cannot be effectively implemented, where policy was not effectively implemented, and generally how closely the systems come to meeting the organization's INFOSEC expectations. Depending on the needs of the client, evaluation can also result in certification and accreditation of systems evaluated.

Key benefits of evaluation include assurance that the systems are enforcing relevant policy, that configurations are having the expected impact, and that weaknesses identified can be ranked for importance and urgency.

Level III: Penetration Testing

Penetration testing is a non-cooperative effort to introduce security failure. Side-effects can be severe, including downtime and corruption or loss of data. These tests have the shortest shelf-life by far, providing a list of successfully-executed attacks into the system, but being unable to assess such issues as policy, procedure, or practice—all critical components of overall information assurance. Penetration testing teams are known as "Red Teams" in military jargon.

Interhack's penetration tests involve several major steps. First, we get clear identification of the target and secure proper authorization from an executive sponsor of the organization involved. Next, the sponsor identifies areas of concern for providing priority to the testing within the defined scope. A set of tests is then constructed and performed, collecting data indicating success of penetration. Depending on the scope of the project, the testing phase is repeated, going a level deeper into the system with each successive pass. An initial report is then released to the sponsor, showing findings, and providing opportunity to raise questions or concerns. Last, a final report is issued, identifying which attacks were most successful against the areas of greatest concern to the sponsor, as well as the effectiveness of any defenses against the attack.

Being the ultimate test of whether the policy and technology are effectively addressing the needs of the organization, penetration tests are the *final* step of a comprehensive information assurance program. Information assurance is a process, the result of policy, technology, and procedure. Just as a runner cannot achieve success by skipping to the last mile of a marathon, an organization cannot test information security by skipping to the last step of an information assurance program.

The key benefit of penetration testing is that after the policy has been defined and assessed and after the systems have been evaluated, the sponsoring organization can see whether the policy and technology for incident detection and response are protecting the organization's assets as expected.

Choose the Right Level

When selecting a service to help your organization achieve and maintain information assurance, your dollar will go furthest by performing these functions in order: assessment, evaluation, and testing. By starting at the beginning and working forward, each level will be able to build upon the previous level, thus providing greater value.

Information assurance is serious business, but it need not be cost-prohibitive. Understanding your needs and knowing which questions to ask a prospective vendor will help you to find a partner who will be able to take best care of your organization and make the most of your information assurance dollar.

C. Matthew Curtin, CISSP, is the founder of Interhack Corporation (+1 614 545 HACK, http://web.interhack.com), a computer experts firm, aiding executives and attorneys facing challenges and opportunities involving the management of information. His work is used to find the right questions to ask and the best answers science can provide. He and his team provide assessment, evaluation, and testing services to support policy definition and enforcement, as well as regulatory compliance in IT. He advises organizations on the use of enterprise-wide cryptographic controls and analyzes information technology and electronic stored information to answer questions that arise in adjudication. Mr. Curtin has appeared as an expert witness in both civil and criminal cases, dealing with everything from electronic discovery to assessment of information technology in practice.

Since 1998, Mr. Curtin has maintained a regular academic appointment as a Lecturer at The Ohio State University's Department of Computer Science and Engineering, teaching courses in the Common Lisp programming language and operating systems. He is the author of *Developing Trust: Online Privacy and Security* (Apress, 2001) and *Brute Force: Cracking the Data Encryption Standard* (Copernicus Books, 2005). Mr. Curtin can be reached at `cmcurtin@interhack.com`.