Information Security Audits

Selecting the right people and targeting them correctly

ARHONT
ANSWERS TO INFORMATION SECURITY CHALLENGES

Introduction

There are several reasons why a company or organisation might decide to order a third party Information Security Audit:

- Management or IT department's proactive approach to security
- Regulatory requirement
- Company audit requirement
- As a post-mortem following a successful break-in

Whatever the reason, Information Security Audits are now a standard task for every organisation. Maintaining an in-house team is impossible for all but the very largest organisations because:

- A dedicated team is required to monitor industry developments
- Staying current requires constant exposure to issues and R&D
- Compliance often demands an independent third-party view
- Maintaining a suitable team is very expensive

In this paper we suggest a process to establish the scope, general approach and priorities for an Information Security Audit, and then how this information is used to select consultants to carry out the work.

Audit vs. Incident Recovery vs. Forensics

The IT security arena is littered with concepts and acronyms. It's worth narrowing our consideration here to three major activities:

- Audit – identifies misconfigurations and flaws that can be corrected before trouble occurs. The IT equivalent of vaccination.
- Incident Recovery – gets the business back up and working after a security problem. The equivalent of surgery.
- Forensics – studies the evidence after a problem to determine weaknesses that need to be addressed. Like an autopsy.

For an Information Security Audit to be effective, the vaccine must be of a high quality and against the specific diseases that pose the most likely threat.

Scoping the Project

To establish the scope of the project we can use a target-based classification to divide the security assessments into external, internal, application, appliance, wireless, physical/social engineering, security policies and related documentation, processes and management controls audits.

Deciding the scope will depend on your work practices, regulatory needs and information security model. For instance, if your company uses a high number of contractors and part-time workers who have access to IT systems and services, an internal assessment should be included in the scope. If the operation of your business strongly depends on a specific application or appliance, an in-depth security analysis of that particular vital asset should be included and prioritised above other tests. In all cases where compliance is involved, security policies, guidelines, procedures, structure, processes and management controls reviews must receive the utmost attention.

Approach

Information Security Audits can be divided along the lines of "how they are done?" and "what is going to be tested?" which results in three types of approach; Black Hat, White Hat and Grey Hat.

A "Black Hat" assessment means that the auditors do not have any access to the checked systems, data and premises, and are supplied the minimal information about the client, such as the company name. Thus, "Black Hat" security assessments emulate a real world external attacker most closely. On the other hand, "Black Hat" testing is not the most appropriate for evaluating the insider threat, and quite a lot of time that could have been spent on in-depth assessment of critical infrastructure and safeguards is devoted to gathering initial intelligence about the target.

As you have probably guessed, the "White Hat" approach is exactly the opposite. The auditors are granted necessary levels of access to the reviewed systems, applications, configuration files, source code, documentation and the company premises. This allows discovery of more security issues and other problems but perhaps isn't indicative of risks posed by real world attackers.

"Grey Hat" testing is a mid-point assessment classification that allows auditors partial or low privilege access to the tested resources.

Skills & Tools Required

With an understanding of the Scope and Approach, you can establish the skills needed. An Information Security Audit requires a wide range of methodologies, approaches, tools and skill sets. Some are purely technical, some demand social manipulation skills, and some a good level of knowledge of information security management, standards, regulations and applicable laws. External auditing, the most common assessment type of today, involves at least a good knowledge of remote access and firewall penetration, as well as IDS/IPS avoidance techniques. Internal audits are devised to counter the insider threat and always require advanced low layer traffic manipulation knowledge, for example, to test VLAN separation and routing/redundancy protocols security. Application testing needs skilful programmers knowing how such applications are written in that particular language; in some cases reverse engineers must be called in. Networked appliances have to be attacked and stress-loaded. Wireless assessments are very complex demanding specialist equipment and detailed knowledge of radio frequency, Layer 2 and wireless security protocols.

Audit the Auditors

Armed with an understanding of the skills required it's time to find suitable auditors. Use the best and most experienced specialists in your technical or other relevant teams to thoroughly examine potential auditors. Demand sample audit reports and pass them to your in-house professionals for a detailed review. Remember, that a proper security audit report should contain not only a sufficient description of a fix for every flaw found, but also a per-vulnerability risk level and attacker skill assessment. There must be a concise summary listing the issues in order of criticality so that you can prioritise follow-on work. There should be clear conclusions outlining your overall security state and providing strategic advice on dealing with general architecture issues, change control, security management and other discovered problems. Not only does this provide essential information for you to act upon, but also helps ensure that the submitted report was not simply an automated document generated by one of the many automated vulnerability scanners.

Looking at certifications can help, although multiple crash courses and boot camps teaching "how to answer questions to pass the exam" instead of applied technical knowledge has undermined even the most trustworthy industry accreditations. To assess their commitment to this highly specialised area, ask the salesman about the Research & Development they undertake; specifically about their contribution to advisories, publications, exploit discovery and tools.

Finally make sure that they not only cover the areas that concern you today but they also have the breadth to cover new concerns that you will have in the future.

Conclusions

A proactive approach to security will always be superior to the reactive one, and periodic audits are an important component of a proactive approach. Choosing the right people to do the job and targeting them correctly will ensure that you get the most from the project.

Dr. Andrew Vladimirov
Arhont Information Security