CS499 Fall 2010 Project :: System Assessment

Due on Wednesday Dec 8th, 2010

Overview

Examining the current infrastructure and practices of an existing organization is one of the best ways of developing skills in assessing its security posture. Students, working either individually or in small groups (**at most 2 members**), select a suitable small- to medium-sized organization. They then interview some key personnel in that organization in order to conduct a suitable selection of security risk assessment and review tasks as it relates to the organization's IT infrastructure and practices. As a result, they can then recommend suitable changes to improve the organization's IT security. These activities help students develop an appreciation of current security practices, and the skills needed to review these and recommend changes.

Turn in: You report in hard copy, in class.

Tasks:

Organization Selection

Students need to first select the organization they will use in conjunction with the course lecturer. It should be of small to medium size, with sufficient people to require a modest internal IT network with internal servers, as well as a connection to some larger external network (e.g. Internet) and some external servers. While it does not have to be an actual organization, it will greatly assist if it is, and you are familiar with it and its IT operations and requirements. Suitable choices of organization might be: a small to medium sized business, a division/unit of a larger business/government department, a school, a university department, or other moderate sized organization. It is important that you obtain permission from your selected organization undertake this type of analysis. While the results can be kept confidential, they can hopefully benefit both parties.

If you have difficlulties to find an orgnization, you can conduct the following task on your own computing system.

Security Risk Assessment

The initial task is to conduct a preliminary security risk assessment for your chosen organization, You may want to use the process described in chapters 16 and 17 of the text. Specifically, the goal is to perform an initial analysis for a combined risk assessment approach. This will involve an attempt at each of these steps:

1. Establish Context and Assets (organizational risk profile and key IT assets)
2. Identify Risks to Key Assets (threats, threats sources, vulnerabilities)
3. Analyze those Risks (existing controls, likelihood, consequence, resultant risk)
4. Assess & Prioritize Risks (document, evaluate, suggest treatment)
5. Develop a Risk Treatment Plan (how treat, possible additional controls)

Given the limited time available for doing this work as an exercise, it will be necessary to limit the time taken and outcomes from this process. The goal is not to conduct a comprehensive assessment, but simply to attempt each step, provide an initial assessment, and to develop an understanding of the issues involved in undertaking this process.

The outcome from this task should be a summary of the context, and an annotated risk register identifying some key assets and significant threats to them. The annotations should identify the reasons and sources for all items in the risk register.

Alternative Subsequent Tasks

Once the organization has been selected, and a preliminary security risk assessment conducted, a selection of the following tasks may be undertaken, as appropriate to the organization of course teaching outcomes. **The outcome from each of these tasks would be a brief report detailing and justifying their findings. At least one of the following must be conducted.**

User Authentication and Access Controls

The student / teams should review the current mechanisms used for IT system user authentication by their organization. Given the outcomes of the risk assessment, you should identify whether changing these mechanisms would be an appropriate

control to improve its security posture. If so, suggest what improved mechanisms could be used, and obtain an indication of the costs involved in their implementation.
Also you should review the categorization of users into groups that may then be used for access control decisions to IT resources. Indicate whether you believe the existing groupings are appropriate, or whether there are better alternatives.

PC / Workstation Security

Given the known problems with import of malware onto client PC's or workstations, the student / teams should review the current mechanisms used to configure and update such systems in their organization, and identify any anti-virus, anti-spyware, and personal firewall products currently used. Suggest whether you believe these mechanisms should be improved, stating your reasons.

Server Security

The student / teams should review the management and security configuration of a key server for their organization. Ideally it should be one identified in the preliminary risk assessment as being subject to a significant risk, and hence needing improved security. You need to decide on which server you will analyze, and detail why it is selected it, and what its importance is to the organization. Then detail the server's security requirements, identifying:

- what information it contains, and how sensitive that information is
- what applications it runs, how they manipulate the information stored, and how critical their availability is
- who has access to the system, and what type of access they have
- who has administrative access to the system, and how this is controlled
- what change management procedures are used to manage its configuration

The student / teams should then detail how they would alter a basic operating system and applications installation process to provide a suitable level of security on this server. They should research ways of installing and armoring the chosen O/S, and the key applications used, to suit their server's security requirements. The information in chapters 23 and 24 in the text will likely be of use.

Network Perimeter Security

The student / teams should review their organization's network perimeter security arrangements, that is their use of firewalls, intrusion detection/prevention systems etc. Given the preliminary risk assessment, you should review what access policy is being used for network traffic across the perimeter, and whether you would recommend changes to it. You should construct a table detailing the network services allowed to or across the network perimeter, of a form similar to that in Table 9.1. You should also state what the default access policy should be (discard or forward), with justification.

You should then suggest an appropriate firewall topology, being one of the options listed at the end of section 9.5 in the text, with details justifying its selection. If possibly, obtain a rough indication of the costs involved in implementing this topology.

Software Security

The student / teams should identify whether their organization uses critical software which is exposed to possible external attack. This would most likely be software running on an externally visible web server to handle responses to forms or other dynamic data handling. You should check what version of software is being used, what the most current version available is, and match this with any reports of known vulnerabilities in this software, as provided by organizations such as CERT, CIO, NIST/NSA, SANS etc. You should detail the threat posed to the organization by any known vulnerabilities, and whether you would recommend this software be upgraded, or hardened in some manner.

Security Policy

The student / teams should review the current organizational security policy. You should correlate the broad structure of the policy with the recommendations for security policy content given in resources such as ISO17799, COBIT, or Information Security Forum (as detailed in section 14.2 of the text). Indicate whether there are any areas not covered in the existing policy that you believe ought to be.