Выполнить перевод на русский язык.

Network Working Group B. Fraser

Request for Comments: 2196 Editor

FYI: 8 SEI/CMU

Obsoletes: 1244 September 1997

Category: Informational

...

1.5 Basic Approach

 This guide is written to provide basic guidance in developing a

 security plan for your site. One generally accepted approach to

 follow is suggested by Fites, et. al. [Fites 1989] and includes the

 following steps:Identify what you are trying to protect. Determine what

 you are trying to protect it from. Determine how likely the threats are.

 Implement measures which will protect your assets in a cost-effective

 manner. Review the process continuously and make improvements each time

 a weakness is found.

 Most of this document is focused on item 4 above, but the other steps

 cannot be avoided if an effective plan is to be established at your

 site. One old truism in security is that the cost of protecting

 yourself against a threat should be less than the cost of recovering

 if the threat were to strike you. Cost in this context should be

 remembered to include losses expressed in real currency, reputation,

 trustworthiness, and other less obvious measures. Without reasonable

 knowledge of what you are protecting and what the likely threats are,

 following this rule could be difficult.

1.6 Risk Assessment

1.6.1 General Discussion

 One of the most important reasons for creating a computer security

 policy is to ensure that efforts spent on security yield cost

 effective benefits. Although this may seem obvious, it is possible

 to be mislead about where the effort is needed. As an example, there

 is a great deal of publicity about intruders on computers systems;

 yet most surveys of computer security show that, for most

 organizations, the actual loss from "insiders" is much greater.

 Risk analysis involves determining what you need to protect, what you

 need to protect it from, and how to protect it. It is the process of

 examining all of your risks, then ranking those risks by level of

 severity. This process involves making cost-effective decisions on

 what you want to protect. As mentioned above, you should probably

 not spend more to protect something than it is actually worth.

 A full treatment of risk analysis is outside the scope of this

 document. [Fites 1989] and [Pfleeger 1989] provide introductions to

 this topic. However, there are two elements of a risk analysis that

 will be briefly covered in the next two sections.

 Identifying the assets

 Identifying the threats

 For each asset, the basic goals of security are availability,

 confidentiality, and integrity. Each threat should be examined with

 an eye to how the threat could affect these areas.