10.7 Documenting Security

By this point, you are undoubtedly aware that you need to document your security. However, you may not be clear as to exactly what documents you should have. Unfortunately, this is an area of network security in which there are no industry standards. There is no manual on documentation.

10.7.1 Physical Security Documentation

A document regarding physical security that is in place should be listed. Where are the machines located? This means documenting the location of every single server, workstation, router, hub, or other device. The documentation should contain serial numbers as well as what personnel has access to them. If a device is in a locked room, then the documentation should also have a list of who has keys to that room.

If you log entry to secured rooms, then copies of those logs should be filed with your other physical documentation. Even in a medium-sized network, this would become a large file quite quickly, rather than a single document. You may consider implementing a certain method whereby after a certain period of time (1 year, for example) the access logs are archived, then after a longer period of time (such as 3 years) they are destroyed.

10.7.2 Policy and Personnel Documentation

All policies must be on file. Any revisions should be filed along with the originals. Assuming you have employees sign an agreement stating they are aware of the policies (and you absolutely should), then copies of that should also be on file.

Along with policy documentation, you should keep a list of personnel along with what items they have access to. This includes physical access as well as any machines (servers, workstations, or routers) that they have login rights to. You should also note what level of access they have (standard user, power user, administrator, and so on).

10.7.3 Probe Documents

Every time a security audit is conducted, a report of that audit should be filed. Even audits done by outside consultants should be kept on file. The audit report should include any flaws found, and have a follow-up report of what steps were taken to correct them.

Should you have a security incident (such as a virus infection or intruder), there should be at least a brief memo summarizing what occurred. That document should state what the security incident was, when it occurred, what machines were affected, and how it was corrected.

10.7.4 Network Protections Documents

The most obvious item to document is exactly what network protections you have in place. This documentation should detail the following:

- What firewall are you using and how it is configured.
- What IDS are you using and how it is configured.
- What antivirus and/or anti-spyware you are using.
- Have you configured any honeypots?
- What individual machine security measures (such as workstation firewalls) have you taken?

One note of caution: These documents should be kept under lock and key, with only limited access. If an intruder were to get access to these documents, they would have a detailed analysis of your network’s weaknesses.