1.9 Approaches of Network Security

Organisations can choose from several approaches to achieve network security. A particular approach, or paradigm, will influence all subsequent security decisions and set the tone for the entire organisation's network security infrastructure. Network security paradigms can be classified by either the scope of security measures taken (perimeter, layered) or how proactive the system is.

1.9.1 Perimeter Security Approach

In a perimeter security approach, the bulk of security efforts are focused on the perimeter of the network. This focus might include firewalls, proxy servers, password policies, and any technology or procedure. These procedure will make unauthorised access of the network less likely. Hardly any effort is made to secure the systems within the network. With this approach, the perimeter is secured, but the various systems within that perimeter are often vulnerable.

This perimeter approach is clearly flawed. So why do some companies use it? A small organisation might use the perimeter approach if they suffer from budget constraints or inexperienced network administrators. This method might be adequate for small organisations that do not store sensitive data, but it rarely works in a larger corporate setting.

1.9.2 Layered Security Approach

A layered security approach does not only mean that the perimeter is secured, but that the individual systems within the network are secured also. All servers, workstations, routers, and hubs within the network are secure. One way to accomplish this is to divide the network into segments and secure each segment as if it were a separate network. This means that if the perimeter security is compromised, not all internal systems are affected. Layered security is the preferred approach whenever possible.

You should also measure your security approach by how proactive yet reactive it is. You can do this by determining how much of the system's security infrastructure and policies are dedicated to preventive measures as opposed to how much are devoted to simply responding to an attack after it has occurred.

A passive security approach takes hardly any steps to prevent an attack. Conversely, a dynamic security approach, or a proactive defence, is one in which steps are taken to prevent attacks before they occur. One example of a proactive defence is the use of an IDS, which works to detect attempts to circumvent security measures. These methods can tell a system administrator that an attempt to breach security has been made, even if that attempt is not successful. An IDS can also be used to detect various techniques

intruders use to assess a target system, thus alerting a network administrator of the attempted breach before the attempt is even initiated.

1.9.3 Hybrid Security Approach

In the real world, network security is rarely inside one paradigm or another. Networks generally fall along a continuum with elements of more than one security paradigm. The two categories also combine in order to form a hybrid approach. One can have a network that is predominantly passive but layered, or one that is primarily perimeter, but proactive. Consider approaches to computer security along a Cartesian coordinate system, with the x axis representing the level of passive-active approaches and the y axis depicting the range from perimeter to layered defence. The most desirable hybrid approach is a dynamic layered paradigm.