Strhuan Blomquist

Abstract

An Intrusion Detection system(IDS) is portrayed as the number one, must have security tool. Vendors claim an IDS can save a company from a lot of plagues like viruses and hackers. A Network intrusion detection system(NIDS) is a network based system that can monitor a network for signs of intruders. This kind of system could also be used to police a network to check employees if they stay within the guidelines set for the network, but is this legal? The questions that need answering are many but the main questions are; are intrusion detection device's really ready for large networks? Have the different IDS vendors adequately addressed the issues brought up in recent years regarding intrusion detection. Maybe the biggest issues with an IDS is; we have an alarm from our IDS, now what do we do?
This paper was written to investigate some of these questions, and to investigate, if any of these vendors actually are creating a complete and competent product that can be an asset to security personnel instead of a burden.

NIDS at the moment seem to create more problems than they solve. The biggest issue at the moment is probably that they give a false sense of security. Other administrators might start to think that they can be more casual about their own security because they got NIDS systems watching their backs. A NIDS also creates an enormous work load for the security administrator to deal with. If they want to use the NIDS to it full potential. The conclusions reached in this paper is that the NIDS vendors still have a long way to go before they will win the hearts and minds of the security community and become an asset.