How Intrusion Detection Works

www.spamlaws.com/how-intrusion-detection-works.html

Intrusion detection is the process of identifying potential threats to networks, computers, databases and other IT devices. Intrusion detection has become increasingly essential with the popularity of the Internet. Many companies have implemented intrusion detection systems to discourage hackers from stealing information and destroying network systems.

Hackers intrude on networks for the purpose of financial gain, industrial espionage, or out of the need to gather attention or protest the apprehension of other hackers. The reasons for hacking are numerous and rapidly increasing as the world relies on the Internet for conducting business and personal use.

Intrusion detection works by collecting information and then examining it for inappropriate occurrences. An IT administrator will use this data to take future preventative measures and make improvements to network security.

An intrusion detection system works by examining the following events:

- **Observing Activity:** The intrusion detection system will observe activity taking place within the network and keep track of user policies and activity patterns to ensure there are no attempts to violate these patterns.
- **Viruses:** Virus and malware can hide within a network system in the form of spyware, keylogging, password theft, and other types of malicious attacks. A good intrusion detection system can spot where they are hiding and then take the necessary steps to remove these hidden files.
- **Vulnerabilities:** When a network system is configured it can create vulnerabilities in system configuration files. In this case the intrusion detection system will identify the vulnerabilities in the configuration files as well as each machine on the network.
- **File Settings:** Authorization files on a network generally consist of a user authorization and a group authorization. The intrusion detection system will check these on a regular basis to ensure they have not been tampered with in any way.
- **Services:** Service configuration files are routinely checked to ensure that the there are no unauthorized services in operation on the network.
- **Packet Sniffing:** Intrusion detection systems check for unauthorized network monitoring programs that may have been installed for the purpose of monitoring and recording user account data activity.
- **PC Check:** The intrusion detection system will check each PC on the network periodically to make sure there have not been any violations or tampering activity. Generally if one PC displays a violation, the system should check all of the other machines on the network.

An intrusion detection system can be run manually but most IT administrators find it easier to automate the system checks to ensure that nothing is accidentally overlooked. It is also necessary to cover all of the bases when it comes to a system check so that statistical analysis can be performed accurately.