ENDPOINT SECURITY

Shri D.Anandam, Instructor Telecom/IRISET

"The perimeter is dead. Abandon your border firewalls and spend your time hardening systems."

As advancement of todays computer network, Information and data is mostly digitised and made online. No human being is exceptional form influence of todays computer networks. Hence, protecting endpoints is most challenging task and cannot depend just on third party solution. Ultimately it is the responsibility of the end-user to protect himself instead of depending on other admin protection arrangements like firewalls, proxies etc.. Risk in computer network is like that even data of standalone PC is not guaranteed from todays malicious activities. Endpoints can include PCs, laptops, smart phones, tablets and specialized equipment such as bar code readers or point of sale (POS) terminals. Each device with a remote connecting to the network creates a potential entry point for security threats. In this scenario, ensuring security is not only responsibility of administrator but also equal responsibility of end user.

As an administrator, a centralized endpoint security suit a part from other security measures should be provided. When a client attempts to log onto the network, the End point server program validates user credentials and scans all possible vulnerabilities in endpoints to make sure that client is up to date with appropriate security patches and complies with defined corporate security policies before allowing access to the network. These suites also use a combination of prevention and detection techniques to identify malicious activity and treat it accordingly by blocking malicious network traffic or preventing malicious software from being executed.

Many of the technologies bundled within endpoint protection software have been available for many years as standalone products or in loosely bundled product suites. Examples include anti-virus and anti-malware software, host-based firewalls (also known as personal firewalls) and host-based intrusion detection/intrusion prevention software. What makes endpoint protection software different from standalone products or loose bundles is that the endpoint protection software components are fully integrated into a single product, with a single interface and management capability. Ideally, all the parts of endpoint protection software work together seamlessly. This creates a solution that is superior to using separate standalone products or loosely bundled product suites..

Most endpoint protection software offers several, but not all capabilities. We should ensure as maximum security capabilities as possible in a given end point security suit. These are some of the features made available as a part of todays endpoint security.

- Antivirus software
- Anti-malware software
- Application whitelisting
- Device control
- Endpoint data loss prevention
- Enterprise mobile device management
- Host-based intrusion detection/prevention systems / Host-based firewalls
- Storage encryption
- Vulnerability assessment
- Patch management

Apart from the above admin side arrangements, the following security measures should strictly be followed by the end user to protect himself from enormous threats of todays Internet.

- Use genuine operating, application and firmware software and ensure they are updated regularly. Better keep automatic update option on.
- Configure PC's personnel firewall properly according to your requirement (i.e. what to allowed and what not to allowed from your system and to your system)
- Disable services which are no being used. This even reduces burdon on CPU.
- Load licensed version of Antivirus software and configure it properly. Preferably load

antivirus with end point security options like malware, IDS/IPS
- Frequently change your admin password which should not be guessable
- Better create a normal user for other than admin activities
- Protect or disable USB ports of your systems
- Scan thoroughly before opening or loading any file or software
- Do not open unknown or doubtable links while browsing Internet.

- Do not use unprotected Internet connections like connections in hotels, airports because they are deliberately not protected. If at all compulsory, use VPN connections or open only web sites starting with https.

Times are changing and information security must change with them. Endpoint security comes down from perimeter to personnel computers give to any chance for any malicious activity at any point of network.