The CYBER GURU

Vong Sopha
Cybersecurity
Analyst

Defense in depth is an approach of safeguarding an organization's network with a series of defensive components so if one layer fails, another will already be in place to prevent an attack. Since there are so many potential attackers with an array of attack methods, there is no single method to assure that an organization's network is completely secure. The defense in depth approach will reduce risk. Some of these defensive components include strong perimeter defense, passwords, and security policies and procedures.

A strong perimeter defense can include a firewall to manage both incoming and outgoing traffic, and deployment of a network intrusion detection system (IDS) to identify scans or traffic patterns that alert in case of an attack. Using strong passwords and frequently changing them can make it more difficult for attackers to guess or crack the passwords. Policies and procedures raise the awareness of users so they will know if their actions are allowed. There is no single security measure that will fully protect an organization's network, but an approach of defense in depth will block or discourage all kind of attackers.