Title:
The Challange - Security Vs. Mobility

Word Count:
652

Summary:
The overwhelming increase in the mobility of the corporate workforce and the availability of wireless internet connections in airports, hotels, and coffee houses, creates an unbearable challenge to IT managers.

Keywords:
mobile security, wireless, Security, Hardware, firewall

Article Body:
The overwhelming increase in the mobility of the corporate workforce and the availability of wireless internet connections in airports, hotels, and coffee houses, creates an unbearable challenge to IT managers. Whenever employees, travelling with their laptops, connect to a hotel hotspot, they are in fact connecting their corporate computers to an unsecured network, shared by hundreds of guests. This innocent connection jeopardizes sensitive data and can bring back security threats into the corporate network when returned to the office. For this reason, IT managers have adopted rigid security policies, creating a conflict between the need for security and the productivity of the mobile workforce. For example, some organizations consider the returning laptops as "infected". The infected laptops are completely formatted and cleaned. Some allow dial-up connections-only (no Wi-Fi), while others go further to completely prohibit the connection of laptops to the Internet outside the corporate network.
This unbearable conflict between security and mobility can only be solved if the mobile force is equipped with the same level of security as they have inside the corporate network. To understand what this means, we should examine the level of security that is maintained inside the corporate networks.

Corporate Network - Two Lines of Defense

Corporate users enjoy higher security levels inside the corporate network because they operate behind two lines of defense. The first line of defense, is a set of robust security appliances, installed at the IT center and exclusively controlled by the IT department. It is largely based on a comprehensive set of IT security appliances running secured and hardened OS, with Firewall, IDS, IPS,

Anti Virus, Anti Spyware,
Anti Spam and Content filtering. The second line is based on the Personal FW and Anti Virus software installed on end-user's computers.
The first line of defense completely isolates the user at the physical and logical layers.
Unlike PCs, these appliances are equipped with a Hardened operating systems that do not have security holes, "back-doors", or unsecured layers. They are designed for a single purpose, to provide security.
The first line of defense provides the following advantages:
- Mobile code is not run - content arriving from the internet is not executed on these appliances it just goes or does not go through into the network. It makes it more difficult to attack as the mobile code delivered by the hackers does not run on the appliances.
Cannot be uninstalled – Security attacks often start by targeting the security software, while trying to uninstall it or stop its activity.
Software-based security solutions, as any software program includes an uninstall option that can be targeted. In contrast, the hardware-based security appliances cannot be uninstalled as they are hard coded into the hardware.
- Non-writable Memory - Hardware-based solutions manage the memory in a restricted and controlled manner. The security appliances can prohibit access to its memory, providing greater protection against attacks on the security mechanism.
- Controlled by IT personnel – The security appliances are controlled by IT, who constantly maintains the highest security policies and updates.
- Performance - The security appliances are optimized for maximum security and operate independently from computers in the network, not degrading the performance of the desktops or consuming their resources.
Consequently, the corporate PCs reside in a secured environment. If the security is breached, at least the damage stops at the gateway. The first line of defense prevents threats from entering the corporate network. While the second line serves as a precaution and help defend against threats that may have already entered the network (e.g. emails). But the real problem starts when the corporate PCs go in and out of this secured environment. Outside the corporate network they are at the frontline with no first line of defense. The problem intensifies as they return, bypassing the first line of defense as they enter the network. These laptops can be considered as the greatest threat because they unknowingly infiltrate security threats
into the supposedly safe network.