ARTICLE ON SKYRECON SYSTEMS INC.
PUBLISHED IN HOMELAND SECURITY ALERT

****

Article Published on 02/15/2008

MULTILAYERED APPROACH FOR PROTECTION AGAINST CYBER THREATS

The increasing number of modern communication tools and services makes the PC infrastructure vulnerable to virus attacks and other cyber threats. These attacks that occur due to various downloads and unauthorized system access are aimed to take complete control over the network operations leading to illegal transfer of monetary and private data, for example. Myriad of companies are involved in developing strong encryption techniques for data security. One such company with efforts towards this direction is SkyRecon Systems Inc. (SkyRecon). Headquartered at San Jose, CA; this organization provides a multilayered approach in its StormShield solution to address the multitude of data security issues.

StormShield is a real-time behavioral solution that is designed and developed to protect PC systems, laptops, workstations, and servers against potential network threats. StormShield employs a single agent to protect an organization's entire set of workstations or PCs from attack. It utilizes a combination of innovative techniques to detect and block all known and unknown threats that may put at risk the security of the systems, communication network and its operating environment. StormShield, complementary to the conventional antivirus software is also integrated with personal firewall. Thus it has the ability to identify and obstruct viruses that pose threat to exploitation of private data and other sensitive content. The firewall integrated in the solution is linked to various violation detection means that facilitates blocking of all communications anticipated to be unsafe and monitors network traffic, thereby providing optimal protection against threats. This solution provides protection against worms, Trojans, network attacks, and pilferage of private information.

StormShield performs all the above defense measures in an automatic manner, that is, without interrupting user activities and tasks. However, it alerts about the blockage of illicit actions or behaviors. The alert that is posted in the corner of the screen provides the option of being activated or deactivated on the users demand. StormShield, a completely protected defense solution is always functional as its key mechanisms are situated within the operating system (OS) kernel, thus being shielded from attack itself. StormShield enables the administrator to define several security policies or behavioral rules, customized to different user groups depending on their business requirement and the type of risks they will likely encounter.

StormShield line of components includes agents, servers, database, and management console. The StormShield agent gets in touch with the server whose function is to hand out and gather security information regarding the workstation. This information that is stored in a dedicated database can be accessed by SkyRecon's management console. The console organizes the StormShield agents, identifies and hands out the security rules, and displays the gathered information. The communication among the components is validated and coded to ensure the proper level of security. An important feature about StormShield is that it blocks threat irrespective of the signature or pattern updates and also does not rely on the user to block new attacks. StormShield's defense ability comprises of intrusion detection module (IDS), which is coupled to the integrated firewall. This IDS aids in scrutinizing the incoming network traffic by deploying a technique called behavioral analysis detection and also facilitates instantaneous filtering of malicious traffic. The combined system and data protection layer ensures security of sensitive data from hackers.

SkyRecon aims to develop customized application solutions that not only recognize the need for true detection but also cater solutions that prevent data loss or data leakage credential. Governments and private organizations need to protect their confidential business data and information, a prime driving factor for network security vendors. SkyRecon recently announced the release of Version 5.0 of StormShield endpoint security, an upgraded version of the existing StormShield. The StormShield version 5.0 deploys multiuser file/folder encryption, thus providing a policy-based secure content encryption model that ensures a wide scale deployment of unified endpoint security solution. Certain additional features of this version include compliance auditing, improved intrusion prevention, enhanced device control, and improved buffer overflow protection. StormShield's integrated secure content encryption, device control, and network access control allows organizations to define a single agent endpoint protection policy that protects sensitive data from intentional and vulnerable attacks. The StormShield dynamic policy model enables businesses to employ and enforce auditable security policies while enabling IT operations and ultimately, business to continue. The StormShield is expected to be commercialized by end of February 2008.