Network Security: 5 Steps to Secure Your Network

Computers are ubiquitous and they abound in networks; it is the network of computers that make organizations live, breathe and operate. Just as exciting and important networks are, given the fact that business profitability and continuity runs deep into the annals of these networks, security becomes just as much critical -- if not more. Security breaches are rampant today and it isn't even about money anymore; sometimes, hackers intrude to soil your reputation.

Business benefits of secure network

If everything pertaining to business functions has to run with the help of computers, networks then, are the hub of most economic activity; not protecting this hub can prove fatal. Among the many benefits of securing business networks, the most importance ones include: to engender customer trust; decrease the costs of data theft, and loss of business resources; to enhance productivity by offering increased mobility with in-built safety (like unshackled Wi-Fi access with security); protecting the businesses against loss or reputation (reputation attacks, for example); allow for seamless business functioning and business continuity and finally, to ensure that the business meets legal norms, compliance requirements (Sarbanes Oxley Act) , etc, that bind down the network security clauses into business workings.

Network Security Threats: What Are We Worried About?

Digital vermin plagues the Internet today and it will be the first point of contact for all business networks to be attacked from -- virus, trojans, mal-ware, Spyware, phishing (and its various forms) attempts, DOS (Denial of Service) attacks and DDOS (Distributed Denial of Service) attacks; reputation attacks, clickjacking and more. As if this wasn't enough you have employees generated problems -- all the way corporate data embezzlement to harmless chatting over unsecured networks -- which are insider initiated and are even more difficult to combat with. Often, businesses also have to deal with zero-day attacks (the latest viruses) which are indeed lethal and we wouldn't even know unless we are attacked.

5 Precise and Practical Steps to Secure Your Network

- **Secure the network infrastructure:** Butler Group had published a report recently which states that companies "*…will look to create a single, managed secure network infrastructure within the next two years, with the market for such services predicted to grow by 15 per cent a year up to 2010*". Protocols like NAC (Network Access Control) are slated to mark this new demand. To secure your network, understand what you are up against and deploy a policy, enterprise wide. Virtualization is an excellent way to deploy a plethora of defensive and even offensive strategies, to combat network threats without the worry of mounting costs, must be implemented; enforce secure physical security to your network at the word go; establish rigid rules and deploy a network security firewall; set-up a VPN(Virtual Private Network for

your mobile employees and use https(hypertext Transfer Protocol Secure and SSH (Secure Shell) and enforce encryption through-out; install proper authentication systems, deploy monitoring of traffic and have systematized auditing processes in place.

- **Secure the Wireless Network, Remote network and Roving users:** The first thing to do when considering wireless networks is the physical security itself -- the Access Points must be within the building and must be tamper-proof (reset buttons can revert the configuration to default values); default SSID must be changed and the "broadcast SSID" option must be disabled; change the cryptography settings; firewalls and all other software used for enabling this network must be updated regularly. Best practices for Wireless Networking like enabling *authentication* and IDS (Intrusion Detection Systems);implementing the WEP Standard, with 128 bit encryption should provide robust security to your wireless network and enable employees to work unhindered by wires and desktops. All of this together with a guaranteed quality of Service (QoS), VoIP connectivity and collaborative software like Cisco meeting Place, WebEx, etc, allows remote-working and enhances productivity.
- **Secure the PC/servers and other Hardware:** Your network servers and PCs can be the source of consternation if adequate care isn't taken to check for any signs of Intrusion. A network-wide implementation of Unified Threat Management (UTM) system; adequate client-side virus protection software -- the best you could find which is constantly updated; Firewalls installed with appropriate configurations (Window XP Internet Connection Firewall (ICF) or any other personal firewalls); Installation of a robust Intrusion Detection Systems (IDS)**;** Updating the Windows Security Patches (to be kept updated constantly); and finally, a rigid application filtering policy to help – filter streaming audio/video, pornographic content, chat software, P2P software, games and other non-relevant data for enterprises.
- **Secure your email:** Email is the ubiquitous messaging medium in businesses today. The fact that most of the spam-ware and mal-ware also enters a network through the same medium shouldn't be so hard to comprehend. Start with a granular, flexible, clear and realistic email security policy; solid Anti-spam, Anti-mal ware and Anti-spy ware software deployment is a must; ensure that you know what you are defending against and do it effectively (you don't want your company to make headlines for the wrong reasons, do you?); make sure that all inbound, out-bound traffic is monitored, including all web mail; Choosing the right deployment for email is critical (SMBs would do well to pick on a "Managed Service" while a " layered Service" can be used by huge organizations; Monitor traffic at all times and ensure that you have a strict policy over images and lastly, invest in compliance to ensure that you have encryption, archiving and reporting best practices in place (Follow The Sarbanes Oxley Act and see the *Cisco's Informational Network* for more information).
- **Have a disaster recovery Plan:** Cisco provides a wonderful approach leading to a flawless Disaster Recovery Plan. Firstly, senior management must take the plunge and formulate a security policy in the company; follow some best practices and these actions should be replicated and systematized across all levels in the company (creates ownership and induces responsibility). The final plan would vary with the company in question but common patterns do emerge: your plan should take some critical factors into account such as the ease of implementing the security plan and the resources it would take; ease of deploying, installing and running the network security protocol; the flexibility of the scope of the network security solution in being

able to allow you t run it satisfactorily, but still prevent it from outsiders; a self-defending network plan can be initiated as a part of this broad policy as an alternative (Cisco's Self-Defending Network Solutions, is a relevant example).

SelectSys LLC
Cisco Certified Partner
Austin, TX
(512) 356-9033
http://www.selectsyss.com

