CYBER Terrorism   How it can impact security in your organization?

Networks today are under attack from an increasingly varied and sophisticated spectrum of virus threats & exploits. We have developed a comprehensive approach to address today's challenge requiring extreme make over in the approach for handling cyber security. The existing security solutions provided by various vendors are only addressing parts of the problem & have not kept up with the evolving sophisticated threats & the impact of social engineering on cyber space. Traditional firewalls are not strong enough to handle today's threats. Inherent computer or software security does not provide proactive protection & not all security tools are created equal. *Computel Systems has developed a unique & comprehensive solution to address today's challenging cyber threats.*

Our four step solution offers "Quad Core Protection"

Step 1   Intrusion/Firewall Protection for Network Security: We recommend a state of the art high performance Next Generation Firewalls as defined by the Gartner group that delivers the critical advanced technology with content filtering necessary to stay ahead of continually evolving threats. Utilizing unique Reassembly-Free Deep Packet Inspection® engine, these firewalls have the ability to scan every byte of every packet and deliver full content inspection of the entire stream with control right down to the individual user s.

Step 2   End Point Protection: This is the most critical area of the protection and this where we will make the maximum impact in maintaining cyber security at your organization. We have teamed up with SYMANTEC to deliver the most effective state of the art cloud based security solution. We can monitor desktop protection at an individual user level with a level of granularity never possible before & alert you before the problem happens. The protection extends to control USB drive access in the systems.

KEY DELIVERABLES

- Simple, fast and effective protection against viruses and malware
- Automates Endpoint updates including patches to provide compliance with security policies
- Available as a cloud-managed service to monitor deployment & report security risks
- Easy setup and web-based management, off loads your IT Department
- Symantec Insight and SONAR technologies detect new and rapidly mutating malware stopping malicious behavior

Step 3   Social Engineering/Training: This is the often neglected part. Phishing is a big problem & the attackers are getting extremely sophisticated in attacking human weakness. About six billion Phishing e-mails are sent each month. We can develop training to suit user profile in your department. The Weakest Link, based on the sheer volume and speed of attacks attributable to unsuspecting employees, it is evident that something must be done to address this issue of cyber security training. Organizations cannot afford to spend increasing amounts of time, money and energy responding to these issues with ever increasing attempts to compromise security. We can help you in providing the right security training for your employees.

Step 4   Desktop Protection: Using proprietary technology we address the vulnerability in a typical Desktop & lock certain functions to prevent hackers from gaining access to the critical parts of your system.

Technical Support & Reporting: Our unique solution includes 24X7 FREE Technical Support for virus related issues & automatically submit weekly/monthly reports for all suspicious behavior at an individual desktop level.

For more information please visit www.computelsys.com

COMPUtEL