

Security

5 Steps to a Secure Infrastructure

The growth of e-business has driven organisations to open their networks to increasingly wide audiences. Communication between these parties, or even the simple use of the vast resource of the internet is essential to remain competitive in the modern business world. But opening your network in this way increases the security risks that your organisation faces.

The threats are very real:

- 44% of UK businesses have suffered at least one malicious security breach in the past year¹
- The average cost of a serious security incident was £30,000¹
- Approximately 90% of security breaches result from poorly configured or unpatched servers²
- Unchecked viruses could cost businesses £907bn world-wide by the end of 2002³

1. dti Information Security Breaches Survey 2002, 2. Gartner, 3. Price Waterhouse Coopers

This is why security is so essential: to ensure that your organisation can remain competitive, yet do so without any concerns about the security, confidentiality, integrity or availability of your organisations systems and its data. Solsis's security solution is comprised of five key steps.

1 – Define A Security Policy

Establishing an effective security policy that defines the security goals of the organisation must be the first priority. A security policy is a formal statement of the rules by which people who are given access to your organisations technology and information assets must abide. It can be as simple as an acceptable use policy for network resources, or it can be many pages in length and detail every element of connectivity and associated policies. Security policies should be reviewed and updated yearly, stored online and made easily available to employees.

2 – Use Effective Authentication

Authentication is the accurate and positive identification of network users, hosts, applications, services, and resources. Standard technologies that enable



identification include authentication protocols such as RADIUS and TACACS+, Kerberos, and one-time password tools. New technologies such as digital certificates, smart cards, and directory services are beginning to play increasingly important roles in authentication solutions.

3 – Implement Perimeter Security

The third step in our solution, perimeter security, provides the means to control access to critical network applications, data, and services so that only legitimate users and information can pass through the network and access its resources.

Routers and switches with access control lists and dedicated firewall devices provide this control. A firewall acts as a gateway through which all traffic to and from the protected network or systems passes and helps to place limitations on the amount and

10 Security Tips

1. Encourage or require employees to choose strong passwords.
2. Require new passwords every 90 days.
3. Make sure your virus protection subscription is current.
4. Educate employees about attachments.
5. Don't just install a firewall – implement a total security solution.
6. Continuously review and evolve your security strategy.
7. When an employee leaves, remove the employee's network access immediately.
8. Implement a Virtual Private Network for secure remote access.
9. Regularly patch your servers with the latest security patches
10. Don't run any unnecessary network services.

type of communication that takes place between the protected network and an external network, (e.g. the internet). A firewall is generally a way to build a wall between one part of a network, a company's internal network, for example, and another part.

Additional tools including virus scanners and content filters also help provide additional perimeter security. Viruses are the most likely form of security breach that an SMB will suffer, and will typically arrive via e-mail attachments. Content filtering allows an organisation to enforce an acceptable use policy, by controlling internet use and monitoring the content that enters and leaves the organisation via the company email system. Content filtering provides the additional benefit of increased staff productivity and network bandwidth.

4 – Virtual Private Networks (VPNs)

Virtual Private Networks (VPNs) connect branch offices and remote users over a shared or public network such as the Internet, with the same security and availability as a private network.

Because VPNs use an existing shared wide area network(WAN) infrastructure, costs are lower and deployment is faster than traditional private networks. Telecommuters, mobile users and branch offices all require dependable access to company networks.

5 – Continuous Monitoring & Management

Hacking tools are becoming increasingly sophisticated and available, but the technical knowledge required to use them is decreasing. As a result, simply implementing a security solution is not good enough – you need to stay one step ahead of the bad guys, which means that you need to continually test and monitor the state of security protection.

Network vulnerability scanners can proactively identify areas of weakness, and intrusion detection systems can monitor and respond to security events as they occur. Results and outcomes from continuous assessment should be used to modify your companies security policy and defence mechanisms as needed.

Solsis Can Help

As a provider of IT security solutions, we can help your organisation stay ahead of the bad guys by helping you to address all of your security issues using the specialist skills, expertise, and resources available at Solsis.

Our security specialists can work with you to provide a range of services including risk assessments, policy development, system design, implementation and security monitoring to name a few.

2007 Preferred Partner



Networking Infrastructure Solutions



UK Partner Qualified for 2007



For further information about these services or other Technology Solutions, please contact our Sales Department on 01344 401548, or visit our web site at www.solsis.co.uk