Editorial Thoughtscapes
Words Impact Business Success
www.et-writer.com

Just A Moment…
IT Commentary

Communications Security

Enterprise security is no longer an option but a necessity. For instance, if you didn't think about security in the past, you certainly need to know the fundamentals about it now. Take communications security as a simple illustration. Before the September 11 terrorist attack, the idea of communications security was a remote consideration. Today, this aspect of security is something on every IT manager's mind.

Yet, there are a lot of complexities to pay attention to when it comes to security. For example, the choices that you typically have involve securing the physical environment within the enterprise. This naturally extends beyond your company's boundaries to the outside world. This involves such activities like intruder detection and contingency for disaster recovery using an offsite backup.

Many of these security processes require a certain skill and know-how competency to plan, implement, monitor and enhance. And such security implementations can be very taxing. Because you are serious about the security plan for your enterprise, you must get started with the implementation process quickly.

But before you do anything, you must assess and decide what you need to secure. Then you need an access policy, and this means authorisation, authentication, encryption, and access controls, and so forth.

In your organisation, you probably have some of the basic security measures in place. These include password and authentication management, firewalls, access controls, and intrusion detection. But the big project such as establishing, and then improving your communications security takes lots of effort, time and money. And continuous monitoring and proactive follow-up.

Many enterprises that have previously neglected communications security now realise that this is now a critical aspect of doing business on the Web. Take a typical scenario. Most enterprises start by creating a secure network tunnel (or VPN) between the employees working inside the company's network and people outside the company's firewall like business partners, or other extranet users.

By creating this VPN, you ensure communications security, and you have the means to manage the connection such that user access is managed securely, i.e., they only go where there are permitted, and do only what they're supposed to do, and hopefully, nothing malicious.

Unfortunately, there is a problem. Most enterprises don't have a good approach on how to create and manage VPNs. There's usually a lot more to making a VPN client than meets the eye. For starters, you need a VPN gateway in your data centre, e.g., a dedicated piece of hardware, or a remote access server, or it can be a function contained within another device such as a router. For an experienced IT person, this should be a breeze as the setting up of some of these devices is not difficult. Yet, it may be beyond the capabilities of many companies, and beyond the staffing levels of smaller firms.

Still, there is one thing that you can do right away that doesn't involve creating your own VPN. Just outsource this job to a security application service provider (ASP). If your company policy allows remote users dialup using a modem, with just a simple login prompt at the remote access server, an offsite VPN service is a quick fix to plug the holes of the unsecured telecom infrastructure. Consult and locate a security ASP that offers such a subscription VPN service. Besides removing the complexities, it may be a more affordable to outsource than implementing on your own.

Since the solution is outsourced, hardware installation is not required except for some software to download, e.g., to a Windows-based machine used as a gateway, and some client software to download for remote users.

A simple solution is nice, yet it is not for everyone. Any viable security solution today has to include a combination of things. Yet, it's difficult to find the best out-of-the-box solution. For instance, a complete communications security may require working with several vendors and involve several different kinds of approaches.

Once a company realises that they have to worry about their own communications security, you will find that they have to do several things at once. They have to assess the risks to their security. They have to look for staff. They also have to look at hardening or strengthening whatever security they already have. The complexity of the process is a good reason why using an ASP for secure communications might be an ideal solution for most companies. This hinges on the outcome of actual service rendered by the ASP, who must simplify the situation, and enable you to get on with your core business.

The truth of the dilemma is that security is no longer simple and straightforward. With the kind of security threats that enterprises encounter, they realise the magnitude of the problem. Today, in the aftermath of New York’s 911 incidence, what may at one time seem so simple to figure out is now a rather complex issue.

One thing is for certain. Communications security like other forms of data security, is even now a basic foundation of doing business securely; and to ensure business continuity in the event of a disaster, a backup recovery plan is just as crucial.

<ENDS>