



Security Essentials

BY IAN HEPBURN

Am I Secure?

“Am I secure?” is probably the most common question I get asked by CEOs in small and large businesses across the Bahamas. According to a 2004 study by The Gartner Group, security remains the top IT related concern among business leaders around the world. And it’s unlikely to change any time soon.

The good news is that most organizations can get secure and stay secure by following a few basic steps.

In Part 1 of my 2 part series on Security Essentials I will focus on the steps you need to take to protect your organization from external threats. In Part 2, I will focus on protecting your organization from internal threats.

Vulnerability Testing

The single biggest security flaw that I see in many companies is that they assume that once they have taken steps to secure their organization then they don’t have to worry about security any more. I call it the “once secure; always secure” myth.

The problem is that new security vulnerabilities and flaws are uncovered every day, leaving your systems potentially open to new methods of attack.

Vulnerability Testing is an absolute must in determining whether your system is still secure from outside attacks. By running a barrage of tests against your firewall, including tests which expose the very latest known vulnerabilities, the idea is to find and eliminate potential holes before hackers find them. We recommend running vulnerability tests at least monthly for all businesses. If your business has particularly sensitive information, more frequent testing may be needed.

Approved Firewalls Only

Like most things, all firewalls are not created equal.

When selecting a firewall for your organization, the single most important feature to look for is whether it meets the industry standard designation of ICSA Labs Approved (www.icsalabs.com). Without this designation, it is not possible to assure yourself that your firewall solution is up to the task of being your organization’s first line of defense.



Virus Protection

If your organization has ever been hit by a virus, you know how much business disruption they can cause. They often result in the loss of critical business information.

Whatever solution you chose, ensure that it meets the following criteria:

- It is ICSA Labs Approved (www.icsalabs.com) as a robust anti-virus solution
- It has been configured to automatically install on all servers and workstations as they are attached to your network
- It has been configured to automatically download the latest virus updates on a daily basis and distribute them to all servers and workstations
- The virus protection status of all servers and workstations can be viewed and managed from a central console

With more than 65,000 known viruses, and new ones being created every day, you simply cannot take any chances.

Prevention is Best

When it comes to securing your IT systems, an ounce of prevention is worth far more than a pound of cure. If you haven't already, take the steps outlined above right away. You'll be glad you did.

To provide feedback on this column, please email makingITwork@providencetg.com

About the Author:

Ian Hepburn is the founder and Managing Director of Providence Technology Group, one of the leading IT firms in the Bahamas. Providence Technology Group specializes in Networking Solutions, Consulting & Advisory Services and Software Solutions.