"Highest Performance
Lowest Price"

Microsoft GOLD CERTIFIED Partner

GFI WHITE PAPER

Security Considerations for Small- and Medium-Sized Businesses (SMBs)

By Brad Dinerman

More than ever, SMBs need to focus on security as part of their IT infrastructure, building around it rather than considering it as an afterthought. This has become even more critical over the past few years as many businesses have unwittingly lost their customers' personal data due to security breaches, and as states and countries have responded by enacting laws to force the businesses to implement additional levels of protection.

From the point of view of this white paper, a small business is any organization that uses between one and two hundred computers, whether servers or workstations. The nature of the business will determine the level of security that is required. For example, a florist will have different needs than a dental office which in turn has different needs than a scientific research center or an elementary school.

Small businesses usually have one or more individuals responsible for the IT and MIS infrastructure within the businesses. While it is all great and wonderful when that individual is trained and has a strong background in IT, there are too many times when the person has been thrown into the position of supporting the systems simply because he happened to be sitting in the front row at the company meeting and volunteered the fact that he configured his own home wireless network.

Whether you are a master of IT or a hapless victim thrown into the role, this white paper will help you identify some of the key areas and issues that you must address in order to maintain a secure organization.

SMBs Need to Peel the Security Onion

"Am I secure?" This question may haunt any SMB owner or IT manager. Yet the question alone does not ask enough information to make an answer possible.

Consider the possible ways that this question can be extended:

- Am I secure against hackers trying to break into my Web server?
- Am I secure against my colleague finding out my password and using my credentials to do something unethical?
- Am I secure against viruses or worms coming in to my system via email?
- Am I secure from the liability of having a student surf inappropriate Web sites?
- Am I secure against an employee copying my sales data onto his USB hard drive or taking away personal, financial information about my customers?
- Am I secure against my server crashing and bringing all productivity to a catastrophic halt?
- And so on, and so on…

Obviously, there are many interpretations of what is meant by "secure." Even if you were able to answer all these questions positively, the nature of technology is such that what is secure today will not be considered secure tomorrow. Ten years ago, I stated over-confidently to my employer that our Windows NT Server running Exchange Server 5.5 was secure. If I were to look at that same system today and again declare that it was secure, then I would be looking for a new career by tomorrow.

Security is implemented in layers. There are many, many layers that need to be secured in an organization. Start at the outer-most layer, peel it away and then find another layer to secure. Peel away that second layer and a third one yet appears. This is what we call the "security onion".

Requirements and Issues Particular to SMBs – IT's All about Budget

I think that it is a safe assumption to state that the single-most important factor that affects a small business' decisions is budget. SMB owners don't usually have hundreds or even tens of thousands of dollars to spend on IT infrastructure. Instead, they look at their checkbook as they hand over their hard-earned dollars to purchase devices such as firewalls to protect their internal network.

"Why," they wonder, "do we really need this? Our new ISP told us that we could just hook up the DSL connection directly to the server and have full Internet access. We weren't expecting to have to pay an additional $400 for a firewall."

Without computer networks, many businesses would just stop functioning. Email goes down and they can no longer communicate with customers. [What's a telephone?] The server goes down and they lose access to the critical database. So why is it that so many small businesses just live day-to-day when it comes to planning for their IT needs? The answer is simple: IT can be expensive. Maintaining and securing it will add even more expense. Businesses just deal with their current needs and hope for the best, and that is often the crux of the problem.

SMBs need to understand that investment in security cannot be an after-thought. It needs to be well-planned, both technically and financially. Without this level of planning, businesses will always be reacting to the latest emergencies, losing money in the process, and never being able to focus on growing the business rather than just repairing it.

So what's an SMB to Do?

So what can you do to enhance the security of your SMB? It's not possible to identify all the areas that need enhancement in a single white paper. However, we can generalize the solutions and place them into two distinct categories: technical tools and procedural/policy changes.

Technical tools

The technical tools are often the easiest to implement, since it's typically a matter of purchasing the right ones and implementing them. Examples include corporate-class anti-virus and anti-spyware software that is installed not just on workstations, but also file servers and mail servers. Most modern firewalls have built-in anti-spyware and anti-virus capabilities; they just need to be activated in order to do their job. But whichever you purchase, make sure that it is current, from a reputable vendor and installed by an individual or organization that truly knows the intricacies of the product. Never accept just the default settings, as they are usually inadequate for any business that values its data.

Email and Web browsing are two of the most typical mechanisms by which malware can be introduced into your network. For example, many messages will claim to come from a trusted source such as Microsoft or your own financial institution, and will contain either hyperlinks to sites that try to collect your personal information, or attachments that the sender claims are needed to "patch" your computer. Similarly, Web sites will often try to deceive you into thinking that you have spyware and will contain a link for you to scan and clean your system, when the fact is that your system was already clean and the software that you will be downloading is the actual malware!

Along with solutions such as firewalls, anti-spyware and anti-virus, it is ***critical*** to educate users about the threats and what they can do to mitigate them. To continue with the previous example regarding fake patches from Microsoft, users should be reminded over and over again that Microsoft and most other major vendors

will never send these updates by email. Rather, they will provide a hyperlink for the user, or preferably the network administrator, to go to the vendor site to manually download the patches.

Procedural/policy

Procedural solutions to improve security are more difficult to manage and enforce. The weakest point in any organization is often the end-user, and as we all know, placing any restrictions on habits which might inconvenience the end-user can result in an unpleasant workplace. None the less, it is imperative to have these in place to protect your organization.

Two examples of policies include:

- Acceptable Use Policy – This is a document that describes what rights employees have with regard to the usage of computer systems. The policy might state, for example, that employees are forbidden to browse gambling or pornographic sites while at work or from any company-owned computer. All employees should sign an Acceptable Use Policy when their employment first begins as well as at their annual performance review. To disregard the terms of the policy can be grounds for discipline or dismissal.

- Remote Access Policy – This provides standards for methods and times that employees may connect to the corporate network from a remote location, including from home and/or mobile devices. Remote access policies can be enforced technically and are important to have in place as a safeguard against improperly transmitting confidential data to insecure or unauthorized sources.

Having policies alone will not provide full security for a SMB. Rather, they will help to minimize the likelihood that breaches will occur by educating end-users and placing potential consequences on their actions.

Conclusion

The SMB market space is just as vulnerable to security breaches as the high-end enterprise. SMB owners or those individuals tasked to provide IT support for the organization must focus on security when building the infrastructure rather than looking at it as an afterthought. Failure to do so will put the company in reactive mode with the potential to lose multiple thousands of dollars in remediation costs, lost productivity and bad press.

Although it's never possible to guarantee that a company is totally secure or that a breach will not occur, implementing the latest tools and providing ongoing, end-user education will minimize those risks and allow you to focus more on growing your business rather than repairing it.

About the Author:

Brad Dinerman is the president of Fieldbrook Solutions LLC, an IT, MIS and security consulting firm in the Boston, Massachusetts area. He is a Microsoft MVP in Enterprise Security as well as a Microsoft Certified Systems Engineer (MCSE), a Certified SonicWall Security Administrator and a Certified 3Com IP Telephony Expert. He even earned a Ph.D. in physics from Boston College, which he claims was "to calculate how long it would take me to launch my frozen computer over the local highway."

Brad maintains his own TechTips site at http://www.fieldbrook.net/techtips/, which has been used by IT support personnel from organizations including NATO, the US Department of Homeland Security, the Department of Energy, the Department of Justice, the US Geological Survey and the Office of Naval Intelligence.

Brad is the founder and president of the National Information Security Group (NAISG, http://www.naisg.org), a member of the FBI's Infragard Boston Members Alliance and a member of the Microsoft IT Advisory Council.