

First Line of Defense

9/29/2006

Ian Burke

Security people so often are not even security people but rather are Networking people or Systems people. Heavens knows that is where I started. I think that is why so often our focus, when we think about security, is on the technical tools. The reality is that when we need to put on our security hat, our biggest tools need to come from our marketing and educational baskets.

The best tools, the strongest piece of armor we have in our network is our user base. It may also be our biggest weakness, but that is ours to shape. Without a strong user support system, it does not matter how secure your firewall is, or how verbose your antivirus software is, you will get penetrated and you will have a breach. Your users have to be educated and they have to be on board with your security program. It is even better if they can be a fundamental part of that program. Either way you need to sell the program to the user base and then educate them on every last part of it.

Let's look at two possible situations. The first, Company A, has a new Cisco ISA firewall with an IPS system in the DMZ. There is a content filter and AV device between the perimeter and the network. Inside the network there is another AV solution and several IDS devices both host based and otherwise. Company A has a NAC solution monitoring ports on the network and generally has very tight security. Employees are frustrated at how limited access is and feel that they are restricted from resources they need to do their jobs. They also lack understanding about the need for the security. Frustration with the system is very high. Due to the nature of business, employees tend to work long hours and often come in on evenings and weekends. Employees have begun to bring in MP3 players, thumb drives, and other media to bypass the network security so that they can get to resources that have been blocked by the IS department. They also have begun to find web sites that provide information that should be blocked but for various reasons bypass the content filter rules. One employee has become so frustrated with the security rules that he has setup a remote sharing session with his home computer and is using that system for internet access. While doing this a hacker has connected to the company systems through that users home system and pulled the company's financials. Two days later the information along with several employees' personal information is on the internet, and people have credit card charges being made on their personal accounts that are not theirs.

Company B is a very different company. It is a large manufacturing company that is struggling to stay open. The management has decided to invest in technology as a way to cut cost, but has limited resources to do this. They are providing computer access for all 7000 employees. For security they initially invest in a Cisco ISA firewall and run Windows authentication off of one of their three servers. They also sit down with all of the employees, by department, and explain how all of the HR and accounting information will be stored on the network along with the other information that they will have access to. They work with the employees to draw up a short term and long term

security plan. They elect a security officer from the production team that will be in charge of monitoring the security system until additional IT staff can be hired. They also coordinate a security committee that will draft up some security policies. The staff is very careful to limit their internet use to strict business use until a more secure environment can be established. Within a short while they deploy a strong AV solution that has been researched by the security team, and the staff is educated on how it works. The company is able to operate with this structure for some time as the entire company has full buy-in to the security policy.

While these are extremes of what can happen, they are both realities in today's world. The point of looking at these stories is that it does not matter what you have for security hardware, your user base will find a way around it if you do not have their support. People today are building web pages, blogging, wiring their homes. I even had a user on my network that had put up a microwave bridge between his house and his barn. The user base is not full of neophytes any more. They are smart, computer literate hacks. In some cases they may know more than we do. We do still have the users that have never used a computer before, and we need to help them along. But we need to be prepared for the entire spectrum. We need their support.