Eight Ways Data Leaks From Your Network

Introduction

What is the single most important component of your business network? Is it your servers, desktops, laptops or phones? They are all important, and some are costly. But if you stop to think about it, the only truly valuable "item" is your data. Everything else can be replaced and if you are well insured, with no more cost than the downtime and aggravation of putting it all back together. Data is not like that. Data is precious, irreplaceable and as you will see, very hard to control.

1. Physical Theft

This is the simplest concept. We all understand theft. That is why we have locks, security systems, cameras, insurance policies and more. These are all "physical" issues and we can protect against them in various ways, from simply placing the server in a locked room to using full-blown access control (card key or biometric) systems. But what if, somehow, these are breached and you find one day that your server is gone? ***Ask NSI about data encryption for your server and backups.***

2. Physical Loss

This is another simple concept with serious ramifications. According to insurance companies, nearly one million laptops are lost or stolen each year in the United States. As incredible as that sounds, nearly 30 percent of cell phones are lost or stolen each year, that's tens of millions! Remember that phones nowadays are often simply small computers that provide data and voice communications and, carry your data. ***Ask NSI about remote wipe, encryption and other phone security issues.***

3. Hacking (Outside Attacks)

This is also a well known, if not well understood, concept. Most of you know that there lurks out there somewhere, millions of frustratingly skillful and determined miscreants just itching for your data. Well, to be precise, not your data per se, but someone's personal information. While it is true that there are few targeted attacks (true industrial espionage), it doesn't take much targeting when you have the numbers these guys have. ***Ask NSI about truly effective firewall solutions.***

4. USB Keys & Portable Devices

Are you wondering about how things like Wikileaks happen? Think of what it takes to move all that data out of a location clandestinely. Chances are it is easier than you think. A single, cheap USB key (drive) can move 32 to 64G of data nowadays. And what about iPods? Did you know they can transport even more than that? USB hard drives – some can hold more than your server! ***Ask NSI about endpoint control solutions to monitor USB and other ports on your network.***

5. Its in the Email

Nearly all of us "live" in our email programs these days. Outlook is open all day long on my desktop, and I rarely go half a day without using it for communications. Of course, we are all very thoughtful about our email communications, never inadvertently sending out sensitive information, attaching a sensitive document or violating any other company policy or regulation in our constant use of our email. ***Ask NSI about email security (antispam) and compliance services and devices.***

6. Instant Messaging (IM)

What is faster than email and twice as hard to control? What can work just like email but leave no traces behind (so much for your compliance issues)? Yes, it is the miracle of instant messaging, whether it be AIM, ICQ, MSN Messenger, or Yahoo. While IM can provide real productivity gains, it can bring danger and wasted time to your office. Did you know that Microsoft offers a managed, reportable, business grade IM solution? ***Ask NSI about controlling and tracking Instant Messaging.***

7. Social Media

What can fritter away more time that YouTube and Solitaire combined? Yes, it is Social Media (aka Facebook, LinkedIn, Twitter, etc.). There is simply no denying the power and importance of these emerging technologies. Like IM above, these technologies threaten both the security and productivity of your business, but very few business can afford to forbid (or worse, ignore) their use. But monitoring and tracking is key. ***Ask NSI about solutions for controlling and tracking Social Media.***

8. Lack of Education

Finally, we have been assuming all along that the first response to each of these issues is technological. But this is putting the cart before the horse. Data leaks from many businesses simply because employees don't know any better. The key here is to put in place procedures, educate your employees and reinforce that training on a regular basis. The very best security system in the world is of little use if the employees leave the doors unlocked.

So put together a real security/data protection plan. Formulate simple acceptable usage policies (AUPs) for your employees, and make sure they understand them (and sign off on them). Train users not to fall for tricks like providing passwords over the phone to strangers, or picking up stray USB keys in the parking lot and putting them in their systems to "see what's on them." Security means vigilance. ***Ask NSI about training your staff in security and data leakage prevention.***

Net Sciences, Inc.

Since 1996, Net Sciences has been building reliable, secure networks for our New Mexico customers. On networks of three to 300 computers, supporting law firms, architects, engineers, scientists, accountants and nearly every other profession, Net Sciences is the complete solution to your business network equation. Net Sciences designs, builds and supports networks, keeping them running smoothly, and protecting your data so that you can focus on taking care of business!