



this issue

The Case for Encryption P.1

Cyberspamming P.2

Upcoming Events
CT Laserfiche
User TrainingJoin us for CT Laserfiche User
Training via the web.

Basic User Training

- Basic scanning
- Organizing and Retrieving
- Processing and indexing
- Viewing and printing

Date: Wednesday, March 30, 2011

Time: 10:00am - 11:00am

Advance User Training

- Advanced scanning
- Import & Export
- Template Creation
- Keyboard shortcuts

Date: Wednesday, April 6, 2011

Time: 10:00am - 11:00am

To register:

Email - register@ctaccess.com

Call - 262-789-8210

Computer Technologies of WI, Inc.
740 Pilgrim Parkway L3
Elm Grove, WI 53122
262-789-8210 ph
262-789-7356 fax
www.ctaccess.com

Scott
Hirschfeld

The Case for Encryption

Encryption technology has been around for a long time and many have used it in some capacity. Often it is a simple zip and password protect of a file, or some sort of secure email program that allows us to encrypt before sending sensitive information.

Encryption is not one of those glitzy, exciting technology topics, but it is one that every business owner should understand. Unfortunately it has become a necessity for many organizations, many of whom don't recognize the risk of not having an encryption strategy in place.

What is encryption? In its simplest form, it is the ability to scramble data so that it cannot be read without the appropriate key set. Encryption comes in many flavors, but the basic rule is that the higher the "bit" number, the better the encryption. 256-bit encryption is a standard today, but as time goes by the standard will move.

Encryption is relevant in relationship to many technology areas. For instance, you should be using encryption on your wireless access point so that nobody can

intercept your traffic and break into your network. A remote VPN connection from home or another office uses encryption to ensure that nobody can read your passwords or data as they are transmitted over the Internet.

The area where encryption has become essential in past years is in protecting data stored on a device in the event of the device being lost or stolen. As devices have proliferated and become more and more portable, the concern is someone getting our data is that much greater. We now have data cached on PCs at the office, laptops with remote workers, iPads, smartphones, flash drives, and more.

Each one of these storage locations represents a risk to your organization. That risk comes in a variety of forms. First, there is regulation. Encryption of some type is required by each of these legislative mandates: Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS), disclosure laws in 44 states, as well as the Fair and Accurate Credit Transaction Act (FACTA), Gramm-Leach-Bliley Act (GLBA), and Sarbanes-Oxley (SOX). Second, there is huge legal liability due to

lawsuits when personal information is lost, leaked, or mishandled. It is important to understand that the information does not actually have to be breached to create financial implications. Just the knowledge of the loss of equipment that potentially has data on it, whether that data is breached or not can create huge costs in notifying people of the loss and potential breach. Finally, a huge risk is that of good faith. If an organization does not have the proper safeguards in place, and there is a problem, the media attention alone can create a devastating loss in good will that could cost customers and even shut a business down.

A potential security issue can come in a variety of ways. For instance, have you ever been working in a coffee shop and made a quick run to the restroom with your laptop sitting on a table next to some guy who looks honest, but...? Airports are notorious for this kind of theft. There are 12,000 laptops lost in US airports every week. Even when sitting in the office, your PC is at risk. A couple of years ago, one of our customers had their office broken into and every PC was stolen off their desks.

The solution to these problems is found in a managed encryption solution. There are a variety of encryption tools out there, and some are even built-in to Windows Server and Windows workstation products. The issue is that if the encryption is not manageable, it becomes cumbersome and ineffective. A centrally managed encryption solution gives an organization the ability to control and implement an encryption strategy for devices located in their office, remote devices, and even for home users. With a solution like this, every data location can be encrypted so

that it requires a "key" to unlock it. This "key" is transparent to the end-user, so they are not bothered by it as long as they have their normal login and password. If the device is lost or stolen, the data is encrypted so that only the appropriate user can reach the data. If by some chance a hacker breaks the login/password security, one would suppose they still would have access to the data. However, with a managed solution, as soon as the unit is reported stolen, and administrator will create an order to revoke the key, or even destroy the data. When the unit checks in over the Internet, it will immediately execute this order and render the device useless and the data unreachable.

A good managed solution will also allow control over flash drives, and optical media. Rules can be put in place to only allow optical media to be used within the organization, and to become inaccessible to anyone outside. A policy within company can also be enforced to require encryption on any USB flash drive. If that USB flash drive is lost and someone else plugs it into their computer, the data will remain encrypted and inaccessible. If someone has reported it stolen, the contents again can be automatically erased when it contacts the management server over the Internet.

Due to the pressures of litigation and compliance, encryption has become increasingly important to organizations handling sensitive data. For more details on managed encryptions solutions and a free whitepaper, please contact me by email or phone.

Scott Hirschfeld at 262-789-8210 or scotth@ctaccess.com



EYE ON IT Industry Trends

Cyberspamming

Symantec reported a sharp drop in spam around Christmas day and an uptrend starting on January 10th. Symantec analysts state the drop from 131 billion spam per day to 47 billion per day was due to Rustock bonet, the world's largest source of unsolicited email being shutdown during these few days. The fake drug ads sent out by the Rustock bonet used as many as 1.7 million pcs. The prediction for 2011 is the spam volume will continue to rise.

To protect your business and customers:

- Unsubscribe to legitimate mailings you no longer wish to receive.
- Be selective about websites you register your email address
- Avoid publishing your email address on the internet
- Do not open unknown email 'attachments or reply to spam.
- Avoid clicking on suspicious links in an email. Type the web address directly into the browser
- Keep your operating system up to date with the latest updates
- Consider using an anti-spam solution