Mountain Computers™ Inc. Newsletter - January 14, 2012

The Best Place in Nevada to take your PC & Business for over 5 years and running!

WRITING - ANDY'S HOW-TO, FROM THE NOT SO OBVIOUS FILE

Years before you decide to earn a PhD, start drafting your dissertation. Instead of stressing for many years and spending tens of thousands of dollars, instead research your PhD dissertation years in advance using the guides, templates that exist on the Internet at various credible and accreditted sources. You have the time now; plan ahead and build a dissertation folder, ideas, notes, research (attributed), and thoughts. Planning ahead removes stress later.
References: http://www.fas.harvard.edu/~wricntr/documents/Thesis.html
http://isites.harvard.edu/icb/icb.do?keyword=k33202&pageid=icb.page138643

COMPUTER SECURITY -- PART IX of X

For nearly 8 years I have watched and monitored the SCADA technology and knew of the threats but held true to not reporting my concern because the Directors and Administrators I knew said there was no worries; unless a flood was caused by an administrator who was on vacation and did not allow others in his staff to adjust dam controls and caused a major 1997 flood. Til this day, SCADA is the choice of remote administration when administered.
"SCADA stands for Supervisory Control and Data Acquisition. These systems were originally created in the 60's on mainframe and mini-computer systems. Today the typical implementation is PLC (programmable Logic Controller) controls and PC's usually connected to a PC Network for centralized data collection." (RM Systems Integrators, 2012) "The term SCADA usually refers to centralized systems which monitor and control entire sites, or complexes of systems spread out over large areas (anything from an industrial plant to a nation)." (Wikipedia, 2012)
The latest in the security risks that have often gone un-noticed or unreported is the attack on SCADA devices that control everything from flood control, energy flow, heating and cooling controls, and more. Remote management and control devices that implement SCADA functionality are usually administered by a vendor or agency that has some knowlege of security other than what the vendor suggests; however, what goes un-noticed is when the vendors or agency computers are breached via VPN or backdoor trojan with remote control access - the SCADA topology is exposed. Network geniuses and hackers alike can take advantage of that security risk and threat. Unfortunately, by the time the threat is noticed, more than what can be expected occurs; exploitation of the extranet or systems architecture of the business. Reference: Wikipedia (2012) - http://en.wikipedia.org/wiki/SCADA
RM Systems Integrators (2012), From the worldwide web: http://www3.sympatico.ca/rmsystems/scada.html

BUILD TO ORDER SERVERS- PART IV

Part IV of build to order servers should include a bit about backups, recovery, software, accounts, and zip ties. The polishing of good server management is the need to have servers with backups built-in and cascaded. Software like Second Copy (gmbh) is a good program to purchase and install. That is your first line of defense past the RAID type of technology implemented, preferrably RAID 10. Then, use Carbonite or some trusted remote backup of critical files. Then, make sure that you are using backup copies of your server software to make necessary installation changes. Never use the original CD/DVDs; those should be put in a safe somewhere with the serial numbers copies and saved inside a secure folder. Lastly, account management, the primary admin accounts should be strongly password protected, a backdoor account added, and no-one, not even the Executive Director or Owner should have Domain Admin or Administrator control within their account. The only accounts that should have full control are the primary domain administrator account, a backup account, or a backdoor account. Lastly, zip-ties. I cannot tell you how often I find servers with zip-ties applied wrongly. Call for more information. Free Quotes available.

TECH TIPS OF THE WEEK

1. Make sure your original software is backed up to image file, along with serial numbers copied to a backup file folder, and only use backup copies of your software to do repairs and maintenance.
2. If you are server administrator, make sure you update your passwords and protect them in the company's safe.

Mountain Computers Inc.
490 E 8th St. Reno, Nevada 89512
Sales (775) 287-9552
Support (775) 324-3524
Office Hours: Mon-Fri: 8am-5pm
Lunch 11x-12x
Saturday 10am-2pm

GO GREEN PC-TUNE UP!

Newsletter designed using Scribus - Open Source and Free