

<< SBS news of the week>>

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2005-03/5658.html>

From: Susan Bradley, CPA aka Ebitz – SBS Rocks [MVP] (*sbradcpa_at_pacbell.net*)

Date: 03/21/05

Date: Sun, 20 Mar 2005 22:50:02 -0800

Kevin's Song of the week

<news://msnews.microsoft.com/#aRCmaJLFHA.2944@tk2msftngp13.phx.gbl>

Blogs of interest

Missed Chad's Sharepoint presentation?

<http://msmvps.com/cgross/archive/2005/03/18/38957.aspx>

SMBaccounting futures?

<http://msmvps.com/cgross/archive/2005/03/18/38914.aspx>

Dana Epp's links to the Security lifecycle

<http://silverstr.ufies.org/blog/archives/000808.html>

Life With Alacrity: Security & Cryptography: The Bad Business of Fear:

http://www.lifewithalacrity.com/2004/02/security_crypto.html

Nice Lab!

<http://www.f-secure.com/weblog/#00000502>

A hack-proof laptop for secret agents and accountants

<http://blog.informationweek.com/windows/archives/002445.html>

Securing wireless LANs

<http://msmvps.com/secure/archive/2005/03/08/37959.aspx>

I fyou haven't installed XP sp2 WHAT ARE YOU WAITING FOR?

Download details: Windows XP SP2 Support Tools for Advanced Users:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=49ae8576-9bb9-4126-9761-ba8011fabf38&DisplayLa>

George Ou » The six dumbest ways to secure a wireless LAN – ZDNet.com:

<http://blogs.zdnet.com/Ou/index.php?p=43>

Security insights

<http://taosecurity.blogspot.com/2005/03/security-insights-from-microsoft.html>

Meet the MSRC

<http://spaces.msn.com/members/msrc/>

Want to meet up with fellow SBSers?

Windows Small Business Server 2003 Partner Group Tour: Microsoft Takes to the Road:

<http://www.microsoft.com/windowsserver2003/sbs/community/usergrouptour.msp>

Kentucky

Louisville

March 21

6:00 p.m.

Michigan

Southfield

March 23

6:00 p.m.

Ohio

Cincinnati

March 22

6:00 p.m.

SMBnation on April 15

Boston

SMB Nation Summits sponsored by HP:

http://www.smbnation.com/smb_nation_summits.htm

Australia SBS Tour

<http://msmvps.com/bradley/archive/2005/03/16/38810.aspx>

In other news

Hackers build back door into iTunes

A trio of independent programmers has released new software that allows people to tap into Apple Computer's iTunes music store and purchase songs free of any anticopying protections. Joined by Jon Johansen, the Norwegian programmer responsible for distributing DVD-cracking code in late 1999, the programmers say their "PyMusique" software is a "fair" interface for iTunes, primarily aimed at

allowing people who use the Linux operating system to purchase music from Apple's store.
http://news.zdnet.com/2100-9588_22-5625991.html

LexisNexis tightens access to personal data
LexisNexis, which last week said intruders had accessed dossiers on about 32,000 people in one of its database products, has restricted access to individuals' Social Security and drivers license numbers. The company's policy shift, which took effect Thursday, follows similar restrictions by a pair of competitors in the data-brokering business: ChoicePoint, which suffered a larger security breach, and Westlaw.

<http://www.siliconvalley.com/mld/siliconvalley/news/editorial/11173693.htm>
<http://www.msnbc.msn.com/id/7231785/>
http://www.usatoday.com/tech/news/computersecurity/infotheft/2005-03-18-lexisnexis-tighter-security_x.htm

Anti-virus vulnerabilities strike again
Users of McAfee's anti-virus products were warned this week of a potentially serious security vulnerability. The bug - unearthed by security researchers at ISS - involves flaws in the processing of LHA files by an antivirus library that gives rise to possible stack overflow attacks. The flaw applies to McAfee AntiVirus Library prior to version 4400.

http://www.theregister.co.uk/2005/03/18/mcafee_vuln/
http://news.zdnet.com/2100-1009_22-5623844.html

Virus writers get stealthy
Virus writers are turning to new tricks as the trend of big-hitting worms eases off in favour of malware that can slip in under the radar. Security researchers have warned that sudden impact viruses, such as the Slammer worm, which cause immediate widespread damage to IT systems are being superseded by slow-burning worms where the focus is on avoiding detection.

<http://news.zdnet.co.uk/internet/0.39020369.39191840.00.htm>

IM viruses increase by 50 per cent a month
<http://www.vnunet.com/news/1162017>

The strange decline of computer worms
Computer worms are becoming less commonplace as virus writers diversify their malware spreading tactics to create the maximum effect for the least possible effort. Email-borne worms, such as NetSky, Bagle and Sober, remain perennial favourites with malware authors but Slammer-style worms are becoming

rarer, according to anti-virus firm F-Secure.

http://www.theregister.co.uk/2005/03/17/f-secure_websec/

Defense's PKI slowly takes root

The Defense Department is getting serious about its mandate that all employees and contractors conduct business through a public-key infrastructure. As Defense agencies work to PKI-enable applications and Web sites, contractors without the digital certificates necessary for operation in that environment are being denied entry, said George Schu, vice president of public affairs for VeriSign Inc. The Mountain View, Calif., company is one of three DOD-approved certificate vendors.

http://www.gcn.com/24_5/news/35268-1.html

Study: Parents use time limits, software to control kids online

Most parents of teenagers who go online say they set time limits on the kids' Internet activity, according to a study released Thursday. They also try to monitor it, in part by placing computers in common areas. Parents also don't shun technical tools. Slightly more than half of parents with online teens — 54 percent — have filtering software installed on home computers, up from 41 percent in 2000, the Pew Internet and American Life Project study found.

<http://www.siliconvalley.com/mld/siliconvalley/news/editorial/11162584.htm>

http://www.newsfactor.com/story.xhtml?story_title=Report---Parents-Filtering-Teens---Web-Surfing&story_id=314

Combating Wi-Fi's Evil Twin

I.T. managers should avoid installing access points that will radiate signals beyond the confines of the physical enterprise. This will make it less likely that hackers can intercept enterprise traffic from the corporate parking lot. Just when wireless hot-spot surfers thought it was safe to get back into the water, hackers have come up with new methods for mimicking corporate Web sites and intranets in the 802.11 environment.

http://www.newsfactor.com/story.xhtml?story_title=Combating-Wi-Fi-s-Evil-Twin&story_id=31469

Decrypting the future of security

At the recent RSA Security Conference in San Francisco, a number of themes predominated and resonated with the record-breaking crowd. As expected, the large software vendors jockeyed for position in extravagant showbiz style. Bill

Gates decided to be merciful and finally put the security product vendors out of their misery by announcing that Microsoft was about to enter their space with a new anti-virus product. They reacted the only way they could: they took it like men and came out swinging, full of jibes and insults.

<http://www.globetechnology.com/servlet/story/RTGAM.20050311.gtkirwanmar11/BNSStory/Technology/>

Report: IRS employees vulnerable to hackers
More than one-third of Internal Revenue Service (IRS) employees and managers who were contacted by Treasury Department inspectors posing as computer technicians provided their computer login and changed their password, a government report said Wednesday. The report by the Treasury Department's inspector general for tax administration reveals a human flaw in the security system that protects taxpayer data.

<http://www.cnn.com/2005/TECH/03/17/irs.computer.security.ap/index.html>

MS: Phishing Bad, Users Complicit, Education Best Defense
Microsoft, along with Trust-e and RSA Security, summarized the plague of phishing attacks as the "fastest-growing form of online fraud," but offered little new in terms of advice or technology. Microsoft Tuesday summarized the plague of phishing attacks as the "fastest-growing form of online fraud in the world today," but offered little new in the form of either advice or technology.

<http://www.informationweek.com/story/showArticle.jhtml?articleID=159900460>

Know your Enemy: Tracking Botnets
In their paper, The HoneyNet Project & Research Alliance, have attempted to demonstrate how honeynets can help us understand how botnets work, the threat they pose, and how attackers control them. The research shows that some attackers are highly skilled and organized, potentially belonging to well organized crime structures. Leveraging the power of several thousand bots, it is able to take down almost any website or network instantly.

<http://www.crime-research.org/news/17.03.2005/1048/>