

<< Small Biz Server news this week – June 18, 2004 >>>

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2004-06/5626.html>

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

Date: 06/21/04

Date: Sun, 20 Jun 2004 22:35:27 -0700

SONG OF THE WEEK

Kevin's song of the week

<news://msnews.microsoft.com/OcmR1HZVEHA.1656@TK2MSFTNGP09.phx.gbl>

BREAKING NEWS

News this week – XP sp2 RC2 is released.....

Windows XP Service Pack 2 Release Candidate 2 Technical Preview Program:

<http://www.microsoft.com/technet/prodtechnol/winxpro/sp2preview.mspx>

<http://www.microsoft.com/downloads/details.aspx?familyid=ef3a35c0-19b9-4acc-b5be-9b7dab13108e>

This spreadsheet lists the full set of Group Policy settings described in Administrative Template (.adm) files shipped with Windows XP Professional Service Pack 2 Release Candidate 2 (RC2).

<http://www.microsoft-watch.com/article2/0,1995,1613667,00.asp?kc=MWRSS02129TX1K0000535>

Microsoft hasn't said much publicly, in terms of the feature tweaks it made between the March Release Candidate (RC) 1 beta of Windows XP Service Pack 2 and the RC2 variant that it made available for download this week. But the company now is confirming our short list of tweaks published earlier this year is accurate.

<http://www.microsoft-watch.com/article2/0,1995,1612867,00.asp?kc=MWRSS02129TX1K0000535>

Microsoft won't be 'done' with Service Pack (SP) 2 once it ships the final late this summer. The company has plans to back-port a number of the SP2 technologies (code-named "Springboard") to other Microsoft products. Microsoft isn't saying much on its plans on this front, but some of its testers are talking.

CHATS AND LIVE EVENTS

The Harry and Andy SBS Chat

June 23, 2004

<http://www.mcpmag.com/chats/default.asp>

Chat: SBS 2003 – Backup and Restore

Description / Abstract: Join experts from the SBS team on June 30th 2004 to discuss tips, techniques, and best practices for SBS backup and restore.

Date: June 30th, 2004

Time: 2:00 – 3:00 PM PDT

Online Chat Site:

<http://communities2.microsoft.com/home/chatroom.aspx?siteid=34000015>

The monthly Executive Circle Security Webcast with Mike Nash, Vice President of Microsoft's Security Business Unit, is a resource to help customers keep up-to-date on security improvements across Microsoft. These webcasts are an opportunity for customers to get the latest details on security enhancements in Microsoft's products as well as tips and insights into key security strategies.

This month, learn more about authorization, authentication and access control for your corporate environment with new details and a live demo of the upcoming ISA Server 2004, Microsoft's next-generation application-layer firewall, virtual private network, and Web cache solution which delivers new levels of security, simplified management and performance. In addition, Mike will report on the latest details of what Microsoft is doing across the company to improve security through guidance, tools, training and technology.

More information and registration are available at:

<http://go.microsoft.com/fwlink/?LinkId=28964>

ANNOUNCEMENTS

In case you missed it Charles Anthe posted this in earlier

Microsoft has identified several issues that occur when installing Exchange Server 2003 Service Pack 1 on Windows Small Business Server 2003. These issues include:

- Outlook Web Access (OWA) now requires a domain to be included when entering a username (e.g. – DOMAIN\username where previously username was sufficient)
- Outlook Mobile Access (OMA) now requires a domain to be included when

entering a username (e.g. – DOMAIN\username where previously username was sufficient)

- The OWA spell check feature now gives an error when attempting to spell check an e-mail from an OWA window.
- A critical alert from the SBS monitoring tools regarding store.exe consuming memory is sent consistently. This alert can be safely ignored, or customers can disable the alert to stop receiving the alert notices.

Microsoft is investigating these issues and will provide an update to our customers that resolve these issues as soon as possible. Customers that need to install Exchange Server 2003 SP1 can do so and work around the issues above.

In other news.....

One in three PCs hosts spyware or Trojans
<http://www.vnunet.com/news/1155923>
...somehow I think that's a right number.....

SPY ACT Wins U.S. Congressional Subcommittee Approval

Consumers who are fed up with being the unwitting recipients of spyware programs may get a break if the SPY ACT becomes U.S. law. The legislation just passed through a House subcommittee on its way to further consideration by Congress. The SPY ACT (Securely Protect Yourself Against Cyber Trespass Act) has been passed by the U.S. House Energy and Commerce Committee's Subcommittee on Commerce, Trade and Consumer Protection. This represents a significant breakthrough in the effort to make the SPY ACT law.

http://www.newsfactor.com/story.xhtml?story_title=SPY-ACT-Wins-U-S--Congressional-Subcommittee-Approval

Senate debates cybercrime treaty

A controversial treaty that is the first to focus on computer crime is inching toward ratification in the U.S. Senate. The treaty would require participating nations to update their laws to reflect computer crimes such as unauthorized intrusions into networks, the release of worms and viruses, and copyright infringement. The measure, which has been ratified by Albania, Croatia, Estonia, Hungary, Lithuania and Romania, also includes arrangements for mutual assistance and extradition among participating nations.

Survey Finds Enterprises Deploying Strong WLAN Security

Large enterprises are aware of -- and are taking action to prevent -- potential security threats

to their wireless LANs, according to a survey released Thursday by iGillottResearch. The survey of 804 IT managers working for large enterprises found that 86 percent of the companies have deployed WLANs. Only two percent of those networks are unsecured, the survey found.
<http://www.mobilepipeline.com/showArticle.jhtml?articleID=22100319>

IP phones can create network security risk
The increasing adoption of Internet telephony may be opening up a significant security risk for companies. While mobile telephone viruses have been the subject of headlines recently, IP-based telephones could represent a more immediate security threat for many businesses. "Attacks on IP phones are actually quite frequent," said Roy Wakim, convergence solutions manager at Avaya South Pacific. "Security is a major issue."
<http://news.zdnet.co.uk/internet/security/0,39020375,39158003,00.htm>

Attack of the zombies
Almost summertime, and the living is easy—unless you happen to be an IT worker employed in any kind of security-related capacity. In that case, it was just new kinds of trouble this week, as worms, hacker attacks and other threats made life miserable. The biggest of the headaches was Tuesday's attack against Web infrastructure company Akamai, which knocked Yahoo, Google, and various Microsoft and Apple Computer sites offline for at least part of the day.
http://news.com.com/Week+in+review%3A+Attack+of+the+zombies/2100-1083_3-5238409.html

Cisco upgrades to help networks defend themselves
Cisco is taking the next step in making its vision of a "self-defending network" a reality. On Monday, the company plans to announce new capabilities in its routers to help protect corporate networks from viruses and worms, two sources close to the company confirmed on Friday. The release is the first phase Network Admission Control (NAC), a collaboration program between Cisco and antivirus companies.
<http://zdnet.com.com/2100-1105-5239359.html>

Wal-Mart Plowing Ahead with RFID
Wal-Mart intends to expand its RFID program in mid-2005 to three additional distribution centers that cover 100 more stores than the pilot. In the fourth quarter, seven more distribution centers — covering 350 stores — will be added. Compliance

lags. Standards disputes abound. Security concerns grow. Still, Wal-Mart has reaffirmed its commitment to its January 2005 deadline for going live with its pilot RFID implementation.

http://www.newsfactor.com/story.xhtml?story_title=Wal_Mart_Plowing_Ahead_with_RFID&story_id=25443

The network strikes back: Experts worry about tech retaliation
In war, politics and sports, it's often said that the best defense is a strong offense. But the foot soldiers of computer security work differently: They scramble to build virtual walls that can blunt the impact of attacks. Now, a Texas company wants to bring vigilante justice to cyberspace.

<http://www.siliconvalley.com/mld/siliconvalley/news/editorial/8957335.htm>

http://www.usatoday.com/tech/news/computersecurity/2004-06-19-hackavenge_x.htm

Complacency is a serious security threat
Identity theft, phishing and new forms of hacking and virus creation are growth crimes. And the levels of sophisticated encryption available to a very wide range of fraudsters is already presenting huge challenges to crime detection agencies. Business has responded to these fears by spending on software. Computing's annual Image Trak survey has shown that security is the number one spending priority for IT decision-makers year after year.

<http://www.vnunet.com/features/1155984>

Asleep at the wheel?

When it comes to beating back hackers, too many companies are still asleep at the wheel. Set up to guard against old-style black hats, their defenses have ignored a newer class of sophisticated attackers who take advantage of Internet back alleys and technology loopholes to penetrate corporate networks. Old-style hacking attacks were direct brute-force affairs: I found some information about your network. Then I went poking around and effectively jiggled the doorknobs of various systems to find an entry point and something worth stealing.

http://news.com.com/Asleep+at+the+wheel%3F/2010-7355_3-5236728.html

Feds, Private Groups to Educate Consumers About Phishing Scams

The federal government and some of the nation's leading consumer organizations and financial institutions today kicked off a campaign to educate consumers about the growing threat posed by "phishing," a sophisticated form of identity theft conducted via e-mail and counterfeit Web sites. Visa USA, the Federal

Trade Commission, the Better Business Bureau and the other coalition members said they plan to work together to teach consumers how to avoid phishing scams and to report suspicious e-mail to authorities.

<http://www.securityfocus.com/news/8936>

Wardriving for WLAN security

The 4th Annual Worldwide Wardrive (WWWD) is under way this week, with volunteers scanning the airwaves in a neighborhood near you for wireless LAN access points.

This year's WLAN discovery effort began June 12 and runs through June 19. The WWWD is organized by a mixed group of security professionals and hobbyists who cruise areas to document the location of access points and how many of them have even minimal security. The goal is to boost awareness of the need to secure residential and corporate WLANs.

<http://computerworld.com/securitytopics/security/story/0,10801,93887,00.html>

No Title:

<http://www.worldwidewardrive.org/main.html>

Index of /tools:

<http://www.michiganwireless.org/tools/>

Akamai now says it was targeted by DDoS attack
Akamai Technologies Inc. said today that problems it experienced yesterday morning were caused by a "sophisticated" and large-scale attack aimed at specific Akamai customers, not by a global attack. In a statement released this morning, Akamai also said the impact of the distributed denial-of-service (DDoS) attack had been overstated. According to Akamai, less than 1% of the company's 1,100 customers "had a significant impact affecting more than 20% of their users."

<http://computerworld.com/securitytopics/security/story/0,10801,93862,00.html>

<http://www.siliconvalley.com/mld/siliconvalley/news/editorial/8938238.htm>

<http://www.securityfocus.com/news/8920>

Security experts ponder Akamai attack, defense

That's the question some security experts are asking in the wake Domain Name System problems at Akamai Technologies Inc. yesterday that resulted in performance degradations for some customers. The company initially said the problem appeared to stem from a broad global Internet attack. But today Akamai said the problems resulted from a denial-of-service attack aimed at four specific customers.

<http://computerworld.com/securitytopics/security/story/0,10801,93874,00.html>

microsoft.public.windows.server.sbs: << Small Biz Server news this week – June 18, 2004 >>>

Q&A: Tom Leighton, chief scientist at Akamai

He talked about the nature of yesterday's apparent DDoS attack

<http://computerworld.com/securitytopics/security/story/0,10801,93875,00.html>

'Zombie' PCs caused Web outage, Akamai says

http://news.com.com/%27Zombie%27+PCs+caused+Web+outage%2C+Akamai+says/2100-1038_3-5236403.html

Russian hackers attacked Akamai servers

<http://www.crime-research.org/news/17.06.2004/435/>

Akamai Web Sites Under Attack

http://www.newsfactor.com/story.xhtml?story_title=Akamai-Web-Sites-Under-Attack&story_id=25420

BCC folks... it's what it's there for...

SurfControl distributes email mailing list

SurfControl yesterday issued an exciting press release outlining "the dangers facing businesses who do not protect their e-mail communications against confidential data loss". As is the local custom, the release was sent by email to a long list of eager recipients. Sadly, the operative responsible has clearly never considered protecting their email communications against confidential data loss by using the handy blind copying facility.

http://www.theregister.co.uk/2004/06/16/surfcontrol_confidential_data/

<http://management.silicon.com/smedirector/0,39024679,39121419,00.htm>

--

<http://www.sbslinks.com/really.htm>