

microsoft.public.backoffice.smallbiz2000: << Small Biz Server news the week of June 6th 2004 >>

<< Small Biz Server news the week of June 6th 2004 >>

Source:

<http://www.tech-archive.net/Archive/BackOffice/microsoft.public.backoffice.smallbiz2000/2004-06/0381.html>

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

Date: 06/07/04

Date: Sun, 06 Jun 2004 22:37:01 -0700

News this week...

Kevin's song of the week

<news://msnews.microsoft.com/uCNONswSEHA.4016@TK2MSFTNGP10.phx.gbl>

=====
And Happy Birthday Kevin!
=====

Smallbizserver.Net > Forum:

<http://www.smallbizserver.net/Default.aspx?tabid=154>

<http://www.microsoft-watch.com/article2/0.1995.1607371.00.asp?kc=MWRSS02129TX1K0000535>

Microsoft is counting on a raft of new community-building tools and technologies to help boost customer satisfaction.

Check out her post on the changes in store... sounds cool!

Next week is "patch week"

And Microsoft now has Security bulletins via RSS feeds --

<http://www.microsoft.com/technet/security/bulletin/secrss.aspx> I now have this feed in Newsgator to "push" me the bulletin info.

Why is XP sp2 such a big release? Joe Wilcox talks about it on his blog

<http://msmvps.com/bradley/posts/7665.aspx>

Microsoft business solutions reorganization

<http://www.microsoftmonitor.com/archives/003052.html>

and you want to know why you need to monitor web surfing?

Scoble: 18.8% of US Web surfers visit porn sites, 5.5% visit search engines (from: IT Facts.biz):

<http://www.kunal.org/scoble/archives/002210.html>

<< Small Biz Server news the week of June 6th 2004 >>

SMB Nation Annual Conference

Seattle, September 10-13, 2004

Are you going to be there in September?

Anne Stanton and I will be!

<http://www.smbnation.com/conference.htm>

In other news.....

Wardriver pleads guilty in Lowes WiFi hacks

In a rare wireless hacking conviction, a Michigan man entered a guilty plea Friday in federal court in Charlotte, North Carolina for his role in a scheme to steal credit card numbers from the Lowe's chain of home improvement stores by taking advantage of an unsecured wi-fi network at a store in suburban Detroit.

<http://www.securityfocus.com/news/8835>

Windows XP Bedevils Wi-Fi Users

<http://www.wired.com/news/technology/0,1282,63705,00.html>

Study: Web porn entices far more surfers than search

http://www.usatoday.com/tech/webguide/internetlife/2004-06-03-popular-porn_x.htm

http://money.cnn.com/2004/06/04/technology/porn_search.reut/index.htm

'Potter-mania' fuels spread of NetSky-P

The frenzy surrounding the latest Harry Potter cinematic offering is helping to keep the prevalent NetSky-P worm alive. Almost three months on from the first sighting of NetSky-P back in late March the worm still poses a significant threat. El Reg inboxes are bombarded with hundreds of copies of the worm each day and we're far from alone. AV firm Sophos places NetSky-P as the second most common irritant last month, second only to the infamous Sasser worm.

http://www.theregister.co.uk/2004/06/04/netsky-p_harryp/

<http://www.vnunet.com/news/1155604>

<http://www.washingtonpost.com/wp-dyn/articles/A15187-2004Jun4.html>

NetSky still dominates virus hit parade

<http://www.globetechnology.com/servlet/story/RTGAM.20040604.gtvirusjun4/BNStory/Technology/>

Korgo Worm on the Move

http://www.newsfactor.com/story.xhtml?story_title=Korgo-Worm-on-the-Move&story_id=24407

Cell phone cameras getting day in court--or not

The administrative office for the federal judiciary is now deciding whether cell phone cameras should be allowed in courtrooms, a source said Friday,

raising the possibility that the popular devices will be banned from yet another place. Recording devices of any kind are usually banned from inside courtrooms. One of the myriad reasons involves protecting the identity of confidential witnesses or of minors accused of crimes. Courtroom personnel fear that cell phones with embedded cameras, not to mention those with both cameras and video recording capabilities, could be put to use without detection.

http://zdnet.com.com/2100-1105_2-5226912.html

Zombies may spoil Microsoft's spam plan

One of Microsoft's plans to fight the spam epidemic is unlikely to adversely affect spammers or reduce the quantity of spam, according to security experts. Microsoft's chairman Bill Gates has been calling for the IT industry to work together and eradicate the spam problem. About six months ago he unveiled an initiative called Penny Black, which was a method for reducing a spammer's ability to send large volumes of unsolicited e-mails using Hotmail and MSN accounts.

http://zdnet.com.com/2100-1105_2-5226548.html

ITU to hold spam summit

<http://www.vnunet.com/news/1155617>

Net Rivals Embrace to Fight Spam

<http://www.wired.com/news/infostructure/0,1377,63708,00.html>

RIAA wants your fingerprints

Not content with asking for an arm and a leg from consumers and artists, the music industry now wants your fingerprints, too. The RIAA is hoping that a new breed of music player which requires biometric authentication will put an end to file sharing. Established biometric vendor Veritouch has teamed up with Swedish design company to produce iVue: a wireless media player that allows content producers to lock down media files with biometric security.

http://www.theregister.co.uk/2004/06/04/biometric_drm/

Linksys Wi-Fi router vulnerability discovered

Cisco Systems has issued a patch for a security flaw in one of its Linksys routers that could give hackers access to consumers' home networks. Alan Rateliff II, an independent security consultant, on Friday said he discovered a vulnerability in the Linksys WRTS54G 802.11g wireless router. The flaw gives hackers a free pass into the Web-based

configuration page of the router when the firewall function is turned off.

http://zdnet.com.com/2100-1105_2-5226918.html

Network Associates warms to behaviour blocking
Network Associates yesterday announced plans to offer intrusion prevention alongside conventional anti-virus software. The move is something of a watershed for the AV industry with a top-tier vendor acknowledging that conventional AV scanning software alone fails to defend against fast-spreading Internet worms like Sasser and Blaster. Conventional AV technology is inherently reactive and leaves a 'Window of vulnerability' where firms can get hit even if they have the latest AV signature updates, Metnetwork Associates acknowledges.

http://www.theregister.co.uk/2004/06/04/mcafee_debuts_behaviour_blocking/

IT security faces Olympian challenge

If all goes according to plan, the only Trojan Horse causing trouble in Athens this summer will be the one in the Hollywood blockbuster Troy. But with 10,500 computers, 450 servers, 450 Unix boxes, 4,000 results terminals and a predicted 200,000 security alerts a day, the IT organisers face an Olympian challenge of their own.

<http://www.itweek.co.uk/Comment/1155619>

Vendors, VARs Embrace Endpoint Security

It's no secret that remote users are among the most common sources of enterprise attacks. Mobile employees pick up viruses and worms on the road, then infect the corporate network when they access remotely through a VPN or plug in at the office.

http://www.crn.com/sections/security/security.jhtml?articleId=18842878&_requestid=72835

Part III: Insider theft and the role of regulation

"Truth be told, everything we've done in the area of extrusion prevention is because of industry regulations. The police were useless in our last extrusion event, and we're developing our self-audit and control capability in order to protect our customer records and actuarial data." "We don't invest in extrusion-prevention technology because it's a criminal offense when one of our employee extrudes critical filings. We feel the legal deterrent is sufficient."

<http://computerworld.com/securitytopics/security/story/0,,93624.00.html>

Security cert body gives lesson in insecurity
Security certification and training body (ISC)2

has apologised for a serious security breach which saw the personal details of thousands of respondents to a survey posted onto an insecure server. Phone numbers, email and contact addresses for many of the estimated 20,000 respondents to (ISC)2 Constituent Survey were easily available on the site because of lax security for a short time towards the end of last week.

http://www.theregister.co.uk/2004/06/03/isc2_survey_snafu/

Tests to uproot Windows passwords begin
Microsoft and RSA Security on Wednesday started beta testing a product designed to phase out the use of traditional passwords and replace them with automatically generated passwords from a SecurID token. SecurID is one of the most popular two-factor authentication systems and is already used by many large enterprises. The token is about the size of a matchbox and generates a new six-digit code every minute.

<http://zdnet.com.com/2100-1105-5225434.html>

<http://news.zdnet.co.uk/internet/security/0.39020375.39156548.00.htm>

Recognition keys access

http://www.trnmag.com/Stories/2004/060204/Recognition_keys_access_060204.html

Back to central patching?

In a new study, officials at the General Accounting Office say the federal government must deal more aggressively with the growing volume of software security patches that overwhelms the ability of agencies to manage. A report on the study released this week describes uneven patch-management practices across the federal government and recommends two changes in the status quo.

<http://www.fcw.com/fcw/articles/2004/0531/web-patch-06-03-04.asp>

For Mac security, communication is key
When it comes to security, Apple Computer's report card reads like that of a gifted child: high marks for achievement, but needs to communicate better with others. In general, the Mac operating system has seen far fewer bugs than its Windows counterpart. But some say a recent vulnerability demonstrates that the notoriously tight-lipped company must communicate more openly on security issues and move more quickly when it comes to plugging holes.

http://zdnet.com.com/2100-1105_2-5225115.html

Open source: Prepare for attack

Do you need open-source legal protection any more than you need meteor insurance? Don't dismiss the idea. Most legal observers discount the legal claims by SCO as illegitimate. But there are bigger challenges to contemplate than those from SCO. In fact, users face a convergence of issues that may ultimately lead to other claims being brought against Linux and open-source software.

http://zdnet.com.com/2100-1107_2-5225405.html

Are developers stealing code?

Many software developers regard 'code-borrowing'—reusing existing software in their own work—as an acceptable practice, despite the legal minefield it could create for their employers, says research due to be published later this week. The anonymous online survey of more than 3,000 developers found that almost 70 percent of respondents keep a personal library of code that they freely carry between employers. Such code is generally used without the lawful owner's knowledge or permission, according to IT legal experts from out-law.com.

<http://zdnet.com.com/2100-1105-5225468.html>

Security starts with developers

<http://www.vnunet.com/news/1155593>

Careless coders tempting legal troubles?

http://news.com.com/Careless+coders+tempting+legal+troubles%3F/2100-1008_3-5226035.html

Wireless Attacks and Penetration Testing (part 1 of 3)

The very idea of a wireless network introduces multiple venues for attack and penetration that are either much more difficult or completely impossible to execute with a standard, wired network. Wireless networks only know the boundaries of their own signal: streets, parks, nearby buildings, and cars all offer a virtual "port" into your wireless network. This is the first of a three part series on penetration testing for wireless networks.

<http://www.securityfocus.com/infocus/1783>

--

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