Computer News for Law Firms

No. 23 | Heckman Consulting llc | Fall 2002

Microsoft Security: an Oxymoron?

New security breaches in Microsoft products are revealed with distressing regularity. Aside from dealing with the concretes, this also raises more general issues: why is Microsoft unable (or unwilling) to deal with these security issues, and how should a small to medium firm that does not have the resources to devote a part-time employee to security approach this problem? Realistically, to what extent is a small firm actually at risk?

Let us consider the specifics first. The latest security issue is unique in that it does not involve a virus, but an everyday feature of Word, the use of field codes. Word uses field codes for a number of ordinary functions, such as setting the date, or putting the name of a document in a footer so that it is printed with the document. The issue is as follows: someone, sends you a document to be edited. You open the document, edit it, print it, and return it to the sender. Unbeknownst to you, "spy" field codes in the document have inserted documents from your hard drive or server into the document or sent them to a web site. The original sender has "stolen" some of your documents, and there is no way for you to be aware of this. This exploit was first revealed on August 26. To date, Microsoft has refused to recognize the seriousness of this problem, although columnist Woody Leonhard reports that its PR agency has sent an email to one journalist claiming that a "fix" is in the works (not for Word 97, which Microsoft no longer supports, though). More ways to use this particular field code are being published every day and the potential damage it can do is expanding apace. For example, it was originally thought that the sender of the document had to know the exact name of the document he wanted to steal, but that is no longer entirely true.

The easiest "fix" for this problem is to obtain a free utility by Bill Coan, which you can run against any document to see whether it contains a "spy" field. This is available at http://www.woodyswatch.com/util/sniff or http://www.wordsite.com/HiddenFileDetector.html. If you are already using Payne Consulting's Metadata Assistant, this supposedly also incorporates a fix for this problem in its latest release.

Will This Actually Happen to You?

This is a widely published exploit that does not require any programming skills other than a moderately sophisticated knowledge of Word. It is not and cannot be picked up by any virus scanners because it is not a virus.

Therefore, any deal or case in which the stakes are high enough poses a risk that someone will try to steal sensitive documents. To some extent the question "how likely is it that this will happen" is irrelevant, since it only takes a single instance for you to lose a big case, be sued for malpractice, etc. Other types of disaster are not very "likely" either, but you still have insurance to protect you. In this case, the "insurance" is free: get the utility and run it against every file sent to you by anyone outside your firm.

Other Security Issues

The risks posed by Word's track changes function have been recognized for several years, and utilities exist to eliminate the danger posed by metadata. This risk is quite serious and actually happened in at least one instance I am aware of. If you open a Word document that had tracked changes turned on using WordPerfect (or any text editor), you see all the comments and changes. One firm received a document written in Word, opened it with WordPerfect and noted the following comment concerning one passage: "Jim, do you think we can get away with this language." Needless to say, it was trivial for the attorney who opened the document to say in the course of negotiations, "now, you know I won't let you get away with that language."

Again, utilities exist to minimize this danger, and as a matter of policy, documents should never be sent out of the firm without accepting all tracked changes. If you were really paranoid, you could open every Word document in WordPerfect before you send it out into the world to make sure it is safe.

Internet Explorer

Internet Explorer occupies a special place in the pantheon of security risks because it is so tightly integrated into Windows (can you say "antitrust"?.....). In addition to Microsoft products, other software programs are increasingly requiring that Internet Explorer must be installed, even if you don't use it (e.g., PC Law, Amicus Attorney, Summation, and others). IE security breaches will affect you even if you don't use it.

Therefore it is critical to keep IE updated. Unfortunately, Microsoft's "critical" updates are not always reliable and in some cases can lead to re-opening old security holes. A Microsoft knowledge base article notes that one "fix" is to tell IE not to trust content from Microsoft! This gives you control over what you install. To do this, in IE, click Tools | Internet Options | Content. In the Certificates section click Publishers | Trusted Publishers. If Microsoft is listed, click on it and click Remove. In the future, as Microsoft implements its new license provisions that allow it to change the configuration of your PC without letting you know about it, this will be even more important. You may also want to disable the auto-update "feature" in WindowsXP. To do this, go to Control

(Continued over)

About This Newsletter

Heckman Consulting is a systems integration firm specializing in the legal market. John Heckman has 20 years experience in the legal community and is featured as a "Top Tier Technologist" on www.lawcommerce.com. This newsletter is published periodically as a service to our clients and others. For back issues go to www.heckmanco.com.

Contact Heckman Consulting at:
One Fencove Court
Old Saybrook, CT 06475
Tel: (860) 395-0881
Fax: (860) 395-0386
email: heckman@heckmanco.com

Oxymoron? (Continued)

Panel | Administrative Tools | Services and change Auto-Update to manual.

Outlook Issues

The two main ways that viruses spread at the present time are through Internet Explorer and Outlook. Microsoft's response to these issues has been to lock down Outlook through a draconian security patch that serious inhibits Outlook's ability to integrate with third-party programs such as the PalmPilot. You now have to tell Outlook that you do want to do the link and for a maximum of 10 minutes.

If you are using Outlook with Exchange Server, there is a patch that enables an administrator to disable this warning. If you are using Office XP, you might want to get Ken Slovak's utility that lets you selectively re-enable options that Outlook outlaws en masse. See www.http://www.slipstick.com/files/attopt.zip

The standard methods of protecting against virus infection (in addition to an anti-virus program that is updated very often) have been 1) to close the viewer pane in Outlook; 2) never to open an attachment that you are not expecting to receive.

However, with the spread of viruses through IE-related holes, this is no longer sufficient. Even more serious, the newest viruses spread by sending themselves to everyone on your e-mail list. Thus you can receive a virus in what appears to be an e-mail from someone you know.

In response to all these issues, an entire cottage industry has grown up to remedy the security problems with Microsoft products. Two of the best sources are Woody Leonhard's "Woody's Watch" site (www.woodyswatch.com) and his various newsletters, and Sue Mosher's Outlook site, Slipstick, at www.slipstick.com. These are worth checking regularly.

Why Doesn't Microsoft Fix It?

The obvious question is: why can't (or won't) Microsoft fix all these problems? Until recently, Microsoft's main stress was on "ease of use." Since this ease of use was implemented through the same procedures used by virus writers, Microsoft regarded its security holes as features or assets rather than as problems. More recently, Bill Gates announced his goal of providing "trustworthy computing." Aside from whether or not you can take Microsoft pronouncements as good coin, there is a serious structural problem here. To truly eliminate the rampant security breaches, the basic code of Windows and other Microsoft products will have to be re-written from scratch and will almost certainly be incompatible with all previous versions. This is not only a massive undertaking, but likely to engender the major problem that all previous versions of any software you use will no longer work. In short, implementing "trustworthy computing" impinges on Microsoft's ability to maximize its profits, and is therefore not likely to happen.

What Is Realistic?

It is safe to say that a firm which does not require login-passwords is unlikely to take a serious approach to protecting its documents from intrusion on the grounds that "it's too much work." There is a realistic core to this argument: it is too much work for a small firm in the sense that a serious approach to security would require devoting a at least a part-time staff member to it. Yes, you can do this yourself on a haphazard basis, but remember Red Adair's adage: "if you think hiring a professional is expensive, try using an amateur."

Rather than simply ignore the issue, firms might consider hiring a consultant to come in on a regular basis – say, a half-day a month – and go over all new security issues as they pertain to the firm. This could also be an occasion to increase user awareness (there is no substitute for ongoing security and anti-virus training). In addition, the consultant could be "on retainer" so that you get a priority response in the event of a particularly serious new virus attack, or the actual infection of your system. In short, take the "retainer" approach that is similar to the way attorneys deal with having experts or other attorneys specialized in certain areas "on call" so that you know they will be available when needed. ■

Five Years of Computer News

This issue marks the fifth anniversary of Computer News for Law Firms. Many of our articles have been syndicated via the Technolawyer network and reprinted in publications reaching hundreds of thousands of readers. Past articles are posted on the Heckman Consulting web site at www.heckmanco.com. Some are outdated, but those on general topics such as why use Case or Document Management programs still read well. ■

Heckman Consulting llc
One Fencove Court
Old Saybrook, CT 06475

Stamp

Tel: (860) 395-0881 Fax: (860) 395-0386 e-mail: heckman@heckmanco.com Web: www.heckmanco.com