

FW: Microsoft Strategic Protection Program

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2001-10/0014.html>

From: Hughes, Don (DHughes@CHI.OSU.EDU)

Date: 10/04/01

Message-ID: <EB9D36CB6512D411B1ED00508BCF41CC50205A@chims02.net.chi.ohio-state.edu>
Date: Thu, 4 Oct 2001 14:14:11 -0400
From: "Hughes, Don" <DHughes@CHI.OSU.EDU>
Subject: FW: Microsoft Strategic Protection Program
To: NTBUGTRAO@LISTSERV.NTBUGTRAO.COM

I am forwarding this in case anyone hasn't seen it yet.

-----Original Message-----

From: Louise Markham [<mailto:lmarkham@microsoft.com>]

Sent: Thursday, October 04, 2001 1:29 PM

To: Louise Markham

Cc: Katherine Gresham; Dan Shea

Subject: Microsoft Strategic Protection Program

Occasionally, I will email you a news letter or a quick message regarding current events in the Ohio area, product announcements, press releases and so on. Please let us know if you would like for me to include you on the mailing, and especially if you would like to be removed from this mailing list.

Dear Central Ohio IT Professionals,

I wanted to take a minute to make you aware of what Microsoft is doing to address Security. Please take a moment to look this over.

Why Now?

It has become incredibly clear that viruses and worms directed against businesses' systems are increasing in frequency and viciousness. They suffer from downtimes that take their businesses off-line or completely down, sometimes for days. Code Red and Nimda are just the latest two examples of worms that have impacted businesses and the economy, globally.

We can't ignore the fact that this kind of behavior is becoming more prevalent and hostile. Internet security is a worldwide issue that affects not just Microsoft's customers, but also anyone connected to the Internet—no one is immune to the problem. We appreciate the great inconvenience that

NT–Bugtraq: FW: Microsoft Strategic Protection Program

many of our customers have suffered as a result of these recent virus attacks. Though there were many customers who weathered the attacks without serious impact, we recognize that, overall we have not done enough to communicate how to secure customers' Microsoft environments. This is our responsibility.

Every company and individual that uses the Internet has a stake in, deserves, and should expect a secure Internet. The increasing frequency and viciousness of viruses and worms propagating across the Internet means that our customers, the industry as a whole, and specifically Microsoft, have to change the way we think about Internet security. This is not a competitive issue. In fact, we will work with anybody, competitor or not, to help make this transformation. We're all victims to this malicious damage; we aren't the worst but we're not the best in the industry either.

Microsoft has always taken the security of our customers' systems very, very seriously. Security has been a primary focus in our development organization as witnessed by the latest releases of our client and server products. We have the best security response mechanism in the industry. We have also built one of the most secure sets of products in the industry but still, we can do better and we will, starting immediately.

Strategic Technology Protection Program

* Security site that explains our initiative – STPP.

<<http://www.microsoft.com/security/>> <http://www.microsoft.com/security/>

Today we announced the Strategic Technology Protection Program (STPP). This program is Microsoft's commitment to make it easier for you to get your systems secure and help you stay secure moving forward. We are going to take a leadership role to make that happen, focusing on people, process, and products. You can really break the program down into two parts: "Get Secure" and "Stay Secure."

Get Secure

This is a sustained campaign of tools, services and support targeted at helping you secure your Windows networks. These tools and services are designed to get you to a secure baseline and is an expansion of the security efforts we've already implemented. The core elements of the "Get Secure" program are as follows:

* Free Virus Support Hotline – 1–866–PC–SAFETY (1–866–727–2338)

This telephone number is for US customers right now, an international number will be available shortly. This hotline provides free support to ANY customer with virus related issues.

* Security Assessment Offering (MCS/PSS)

This will be available November 1st through MCS/PSS. While this is a comprehensive, fee–based program, you should be aware that your General

NT–Bugtraq: FW: Microsoft Strategic Protection Program

Manager has the option to exercise BIF funds to support key accounts.

- * Microsoft Security Tool kit – October 15 RTM – Shipping

10/22

- * You can access the toolkit TODAY.

<<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/stkintro.asp>>

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/stkintro.asp>

- * You can order the toolkit for free (3 to 6 weeks for delivery).

<<http://wwwprod/security/kitinfo.asp>> <http://wwwprod/security/kitinfo.asp>

- * Provides a one button update to secure systems

- * Server oriented security resources for server administrators

- * Updates for server security

- * Windows NT 4.0, Windows 2000, IIS, IE Service Packs

- * Critical severity security patches and patch rollups

- * Security Tools

- * Security configuration lockdown for web servers

- * Additional protective software for web servers (attack URL blocker)

- * Windows Update bootstrap client for Windows 2000

- * Enterprise Security Tools – December RTM

- * Security configuration scanner (verifies security configurations and patches)

- * SMS security patch roll out tool

- * Windows Update: Auto update client including control of patch selection by group policy

Stay Secure

Stay secure is the second part of the program are tools and services targeted at maintaining systems security once a secure baseline has been attained.

- * Enhanced Product Security – beginning October 25th for client systems with the release of Windows XP

As with Windows XP, greater security enhancements will be incorporated in the release of all new products including the Windows .NET Server family.

- * Windows 2000 Security Rollup Patches – December 2001

NT–Bugtraq: FW: Microsoft Strategic Protection Program

Bundles all security fixes into single patches on a bi–monthly basis and reduces the number of reboots and administrator burden

* Windows 2000 Service Pack (SP3) – February 2002

This SP will provide the ability to install the most recent security patches along with SP3. It will also provide a careful review of the code to address any new problems detected in SP3.

* Federated Corporate Windows Update Program – February 2002

This will allow enterprises to host and select Windows Update content on staging servers.

Security continues to be the very highest level of priority across all areas of product development. Our customers play a pivotal role in that development cycle by providing feedback through processes such as the security design reviews and Chief Security Officer Forums. We're committed to stepping up our engagement through these activities. While we continue to improve our products we are also committed to a long term strategy of process development, education, and consultancy to ensure our customers can maintain their Microsoft environments at the highest levels of security and reliability.

Please let me know if you have any questions, concerns or recommendations.

Sincerely
Louise Markham – US Headquarters Sales Representative
lmarkham@microsoft.com

Microsoft Corporation
One Microsoft Way
Bldg: SAMM E 6452
Redmond, Washington 98052
Telephone: (800) 426–9400 x11808
Fax: (425) 936–7329
Software for the Agile Business. Enterprise Software from Microsoft. *

Delivery co–sponsored by Trend Micro, Inc.

BEST–OF–BREED ANTIVIRUS SOLUTION FOR MICROSOFT EXCHANGE 2000

Earn 5% rebate on licenses purchased for Trend Micro ScanMail for Microsoft Exchange 2000 between October 1 and November 16. ScanMail ensures 100% scanning of inbound and outbound traffic and provides remote software management. For program details or to download your 30–day FREE evaluation copy:

http://www.antivirus.com/banners/tracking.asp?si=53=245=http://www.antivirus.com/smex2000_rebate

NT-Bugtraq: FW: Microsoft Strategic Protection Program

- *Previous message:* Andy Richard: "Re: Microsoft Strategic Technology Protection Program"
- *Messages sorted by:* [date] [thread] [subject] [author] [attachment]