Privacy Audit

Short Report Version 1.0

Target of Evaluation (ToE)

MU6.0 with WSUS2.0

Timing of the Privacy Audit

April 2005 to November 2006

Name and Address of the Applicant

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399
USA

Names and Addresses of the Experts

2B Advice GmbH
2B Secure Evaluation Body for Privacy (Legal)
Head: Marcus Belke, Attorney at Law
Wilhelmstr. 40-42
53111 Bonn
Germany
marcus.belke@2b-advice.com

TÜV Informationstechnik GmbH:
Evaluation Body for Privacy (Technical)
Head: Dr. Silke Keller
Langemarckstrasse 20
45141 Essen
Germany
S.Keller@tuvit.de

Short Name of the IT Product/Service

Microsoft Update Service 6.0 (MU6.0) and Windows Server Update Service (WSUS 2.0) (MU6.0 and WSUS2.0)

Short Description of the IT Product/Service

The ToE – MU6.0 and WSUS2.0 – is a service with which Microsoft offers to the user the opportunity to obtain both updates and upgrades of products of Microsoft. The overall purpose of the ToE is largely set out by Microsoft Update Service 6.0 and is extended by the special features of Windows Server Update Service 2.0.

More Detailed Description of the IT Product/Service

Until recently, Microsoft users have obtained both updates and upgrades of Microsoft products via various sources and/or different websites to which individual products referred either from within the product itself or by means of reference within respective manuals.

In information technology the word “update” is generally defined as an extension which may be installed to improve a program or an entire system to advance to a higher version and/or to rectify errors. An update in the form of a so-called security patch is particularly important as it ensures that security gaps / flaws are closed. Normally, updates are issued by the respective software operator or distributor, and are either subject to charge or free-of-charge, depending on the purpose or the operating system. The updates offered by Microsoft are offered free-of-charge by Microsoft. Via the ToE, Microsoft also delivers software components from third party suppliers. This applies in particular to any equipment drivers offered by the respective Microsoft product. In addition, Microsoft provides optional software products and add-ons to products already owned by the user. Via the Product ID (PID) Microsoft may verify the admissibility of respective licenses of the user. What is more, Microsoft may, in turn, refuse to provide an update/upgrade where verification has shown a respective result.

Basically, MU 6.0 consists of two main components: The service infrastructure that provides the MU service over the Internet, i.e. the “MU Service Site,” and an update client on the client computer that is the consumer of this service.

With WSUS2.0 it will be possible to use one’s own update server. Clients who wish to provide updates only after special tests or who are unable or unwilling to provide a direct access on-line to workstation computers and servers can install this component as an extension of a Windows server with on-line access. WSUS2.0 will then mirror the updates provided by Microsoft. As a consequence, administrative bodies of a private or public legal person can decide for themselves whether or not an update will be offered at all and which updates will be offered to which work stations of a client. By design the WSUS Corporate Instance is much like a copy of the MU Service: The protocol is designed to provide a single unified design optimized for both Client/Corporate Server and Client/Microsoft Update Service communications. For the client computer, the interfaces to the WSUS Corporate Instance are nearly identical to those of the MU service site.

The results of the privacy audit are only applicable to Microsoft Update Service 6.0 (MU 6.0) and Microsoft Windows Server Update Service 2.0 (WSUS 2.0). The products must be used in the following environment:

MU 6.0 client:
Operation systems: Windows XP Home Edition SP2, Windows XP Professional SP2
Internet Explorer 6.0 and higher

WSUS 2.0
Operation systems: Windows 2000 Server SP4, Windows 2003 Server

The user of MU 6.0 and the administrators of the WSUS 2.0 shall assure that client computers and servers are sufficiently protected using virus scanning tools and firewalls against malicious code or direct attacks intending to harm the privacy functions of the TOE.

The ToE does not comprise any of the following services and features:
Product activation/registration, Feedback- (Responses-) procedure, Survey-procedure, Windows Genuine Advantage (WGA), Piracy Report, CD-Order.

Tools Employed for the Production of the IT-Product/Service

- Microsoft Visual Studio.Net Professional 2003
- Microsoft Office Professional Edition 2003
- Microsoft Office Visio Professional 2003
- Microsoft Office Project Professional 2003
- Microsoft Product Studio 2.10
- Microsoft Source Depot 3.0
- Microsoft FxCop 1.3
- Microsoft SQL Server 2000

Purpose und Usage Environment

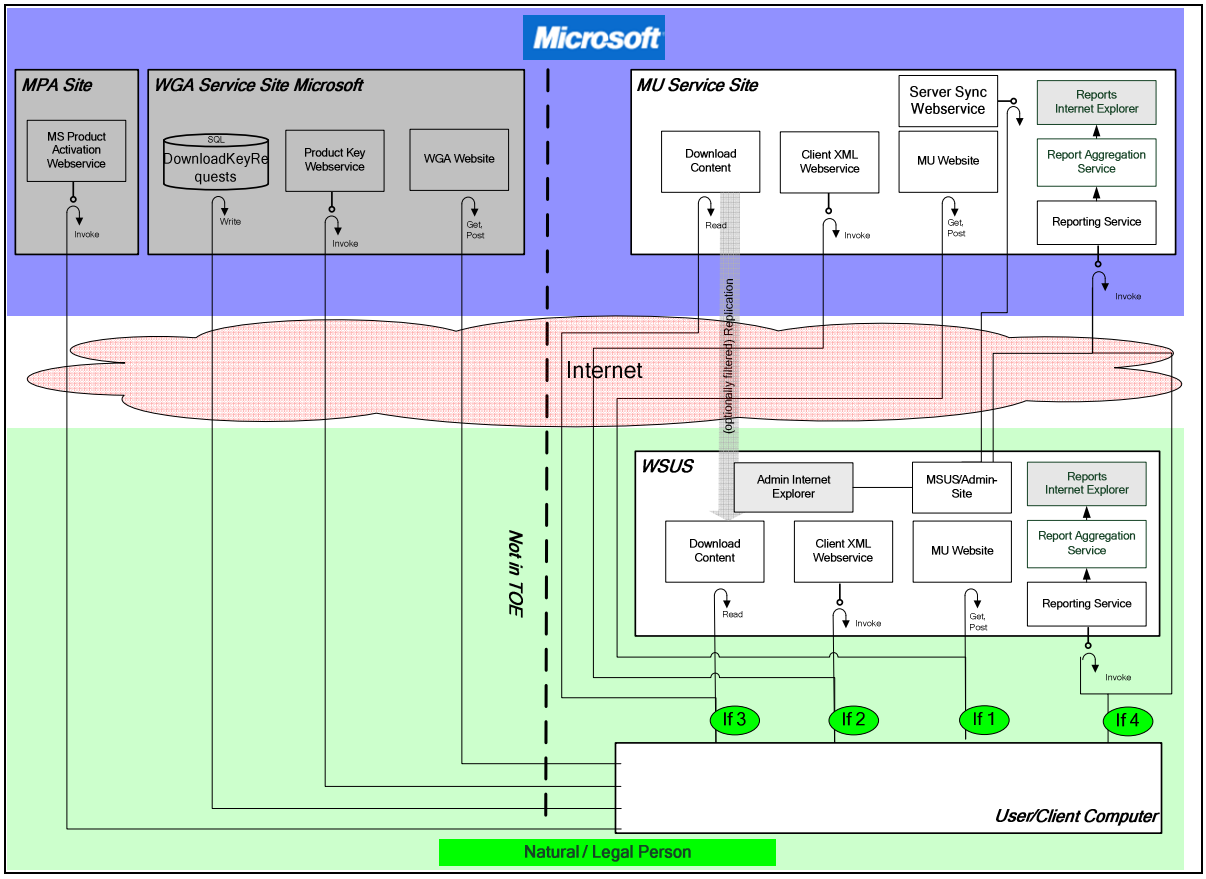
Especially with regard to attacks resulting from programming faults, e.g. buffer overflows, obtaining both specific updating and upgrading software (e.g. security updates, other updates, and improvement updates) is indispensable for a duly functioning of a data processing installation. Thus, the purpose of the ToE is both to maintain and to permanently improve the proper functioning of a data processing installation, and, in turn, to support the IT-security and the data protection strategy of the user. The ToE may be used on both

private (business and non-business) and public data processing installations provided that the following environment is given:

MU 6.0 client:
Operation systems: Windows XP Home Edition SP2, Windows XP Professional SP2
Internet Explorer 6.0 and higher

WSUS 2.0
Operation systems:
Windows 2000 Server SP4, Windows 2003 Server

146 **Modeling of the Data Flow**



147

148 A user/client computer obtains Microsoft Updates either directly from the MU Service Site or
149 indirectly from an intermediary WSUS instance. The client computer connects in the first
150 case via the internet to the MU Service Site and in the second case via a network of an
151 organisation to the WSUS server of the organisation. The WSUS server in turn obtains the
152 available updates from the MU Service Site via the internet and an IT administrator of the
153 organisation manages the distribution of updates from the WSUS server to the client
154 computers.

Version of the Requirements Catalogue, Forming the Basis of the Privacy Audit

Version 1.2

Summary of the Audit Results

TÜV Informationstechnik GmbH (TÜViT), Essen – Member of TÜV NORD Group – and 2B Secure - the Evaluation Body for Privacy of 2B Advice GmbH - evaluated by order of Microsoft Inc., Redmond, Microsoft Update Service 6.0 (MU6.0) and Windows Server Update Service (WSUS 2.0) from April 2005 to November 2006. A legal audit of Microsoft's statements, policies and specifications was performed to set the requirements for a technical audit which, in turn, determined that the program's databases, source code and implementation respect privacy concerns. The realization of the evaluation occurred on basis of documents, statements, and, partly, inspections of the source code. MS has signed the Safe Harbor agreement for human resources and customer data on 29th of June 2001.

The evaluation showed that it is questionable whether the ToE may be considered to collect, process or store personal data. The only situation within the ToE where personal data might be collected and processed is the use of the WSUS part of the ToE where a WSUS-administrator may possibly reference report-system-data of a specific computer, e.g. data concerning Update status, Computer status, Synchronization WSUS configuration settings, etc., to an individual employee by means of the Security Identifier (SID), the string "UserAccountName," and other domain-account-data to which a WSUS-administrator might be assumed to have access.
Even if one followed the stance that, within Microsoft Update 6.0 (MU 6.0), from the point of view of Microsoft, IP-address or PID needed to be considered as personal data, their collection, processing, use and storage would be covered by a statutory permission. The collection of both IP-address and PID is bound to an admissible purpose and erasure is performed promptly. The ToE needs to track and record the number of individual computers that use the ToE to verify whether updates are required and whether the download and installation of specific updates succeeded or failed. Thus, the purpose of the collection, processing, use and storage of both IP-address and PID is to guarantee the proper functioning of a data processing installations of users of Microsoft products and the security thereof. With view to the front end Microsoft keeps the Logs for 7 days on the IIS servers and 30 days on tape. Microsoft does not log the referrer address. With regard to the reporting service IP address information is kept no longer than 3-4 hours. Once Microsoft processes data for a given hour all IP address information is discarded.

In the case of WSUS it is highly questionable whether or not aforementioned report-system data of a specific computer represent personal data within the meaning of section 3 (1) BDSG and section 2 (1) LDSG-SH. Nevertheless, even if these data do represent personal data the collection, use, and processing of which will be covered by statutory permissions. After all, it will be up the WSUS-administrator to design procedures in a way that meets data protection provisions.

With view to employees of the public administration or public officials the collection, processing, usage and storage of aforementioned data may be considered to be covered either by the permission of sections 13(1) BDSG and 14(1) BDSG in conjunction with section 14(4) BDSG or by the respective sections of the LDSG of the Länder, e.g. section 11 (1 Alternative 3) LDSG-SH and section 13(2) LDSG-SH in conjunction with section 13(6) LDSG-SH. With view to employees of non-public bodies the collection, processing, usage and storage of aforementioned personal data may be considered to be covered by the permission of section 28(1 sentence 1 No. 2) BDSG in conjunction with section 31 BDSG.

According to the obligation to instruct, pursuant to section 4(1) TDDSG, the “Microsoft Update Privacy Statement” barely meets the requirements of this section. There is room for improvement, though. Concerning transparency and product description all descriptions as to what to do, and which options are available become clear from the texts on the Website. However, with regard to the “Microsoft Update Privacy Statement”, the user might not be instructed sufficiently on the fact that a cookie will be set on their computer, for how long this cookie will stay on their computer and in which way the user can erase the cookie. Besides, it would be desirable for Microsoft to provide the information that the data is being used and stored in the United States of America and some further information, e.g. by means of definitions and examples since the user might not be able to fully understand certain notions, such as “GUID” or “PID.” However, Microsoft has stated that they have started to address aforementioned issues in an updated “Microsoft Update Privacy Statement” and “Windows Update Privacy Statement.”. The new Microsoft Update Statement will be published by end of march 2007 at the latest.

From the point of view of a local administrator implementing and setting up MU 6.0 with WSUS the administrator guidance provided on the respective web pages and the WSUS online help are suitable to support an administrator in the relevant administration tasks.

What is more, with regard to section 4(4) TDDSG and section 9 BDSG including the Annex to sentence 1 thereof, sufficient technical and organizational measures are implemented to

guarantee that there is no combination of utilization data of different Microsoft Online-Services because Microsoft has set up the service of the ToE as a dedicated Microsoft Online-Service with dedicated servers.

The ToE is in line with the requirements of the principle of data prevention and data economy within the meaning of section 4 LDSG-SH. With view to auditing acceptability the ToE may not provide additional technical means. However, the requirement of auditing acceptability depends on the respective potential for misuse. With regard to the ToE the potential for misuse may be assessed as small considering both the limited possibilities of a WSUS-administrator and the respective types of data which are of minor sensitivity. Eventually, auditing acceptability might be guaranteed by organizational means, e.g. printed copies of reports of the ToE.

Description, How the Products Support Privacy

The ToE provides the following functions that support data protection and privacy:

- user-friendly provision of important updates against new security and privacy threats
- configuration options of scheduling and notification
- integrity protection of update files by electronic signatures and signature verification
- updates to end user clients and to corporate WSUS instances

The WSUS 2.0 part of the TOE provides

- features that administrators need to manage and distribute updates
- updates for various Microsoft operating systems and products
- automatic download of updates from Microsoft Update by product, type and language
- customization of updates to specific target computers and computer groups
- verification of suitability of updates before installation
- reporting capabilities
- flexible scalability for a wide range of organisations.

The product meets the possible technical standards, it does not ask for personal data providing updates, upgrades and free additional software to the user of Microsoft products.
The product's ability to enhance privacy is delimited by IT environment conditions:
The user of the MU 6.0 client and the administrators of the WSUS 2.0 have to assure that the client and the server, respectively, are sufficiently protected using virus scanning tools and firewalls against malicious code or direct attacks which may be used to harm the privacy

functions of the TOE.

Furthermore, a WSUS server has to be installed within an organisation’s firewall.