Datenschutzprüfung
Kurzgutachten Version 1.0

Objekt der Bewertung (ToE):

MU6.0 mit WSUS2.0

Zeitraum der Prüfung

April 2005 bis November 2006

Name und Adresse des Antragstellers

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

Namen und Adressen der Sachverständigen

2B Advice GmbH
2B Secure Prüfstelle für Datenschutz (Rechtlich)
Leiter der Prüfstelle: Marcus Belke, Rechtsanwalt
Wilhelmstr. 40-42
53111 Bonn
Deutschland
marcus.belke@2b-advice.com

TÜV Informationstechnik GmbH:
Prüfstelle für Datenschutz (Technisch)
Leiterin der Prüfstelle Dr. Silke Keller
Gutachter: Stephan Di Nunzio
Langemarckstrasse 20
45141 Essen
Deutschland
s.dinunzio@tuvit.de

Kurzbezeichnung des IT Produktes

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

Kurzbeschreibung des IT-Produktes

Mit der zu untersuchenden Dienstleistung – MU6.0 und WSUS2.0 – bietet Microsoft dem Nutzer die Möglichkeit, Updates und Upgrades von Microsoftprodukten zu erhalten. Der allgemeine Zweck der zu untersuchenden Dienstleistung ist weitestgehend im Microsoft Update Service 6.0 dargelegt und wird erweitert durch die speziellen Funktionen des Windows Server Update 2.0.

Detaillierte Beschreibung des IT Produkts

Bis vor kurzem haben Nutzer von Microsoftprodukten sowohl Updates als auch Upgrades über verschiedene Quellen und / oder unterschiedliche Webseiten erhalten, auf die die jeweiligen Produkte hinwiesen, sei es im Produkt selbst oder in der jeweiligen Bedienungsanleitung.

In der Informationstechnologie wird der Begriff "Update" gemeinhin als Erweiterung verstanden, die installiert werden kann, um ein Programm oder ein ganzes System zu verbessern oder auf den Stand einer höheren Version zu bringen und / oder um Fehler zu korrigieren. Ein Update in Form eines sogenannten "security patches" ist besonders wichtig, denn es stellt sicher, dass Sicherheitslücken und -fehler geschlossen werden. Normalerweise werden Updates vom jeweiligen Softwareanwender oder -lieferanten in Abhängigkeit vom Zweck des Betriebssystems entweder gegen Entgelt oder unentgeltlich zur Verfügung gestellt. Die von Microsoft angebotenen Updates werden unentgeltlich angeboten. Über das zu untersuchende Objekt der Bewertung (ToE) liefert Microsoft auch Softwarekomponenten von Drittanbietern. Dies gilt insbesondere für Gerätetreiber,

die das jeweilige Microsoftprodukt bietet. Zusätzlich bietet Microsoft Softwareprodukte nach Wahl und Zusätze („Add-Ons“) zu solchen Produkten, die der Nutzer bereits besitzt. Über die Produktidentifikationsnummer (PID) kann Microsoft die Echtheit der jeweiligen Lizenzen des Anwenders überprüfen. Darüberhinaus kann Microsoft – je nach Ergebnis der Prüfung - dem Nutzer ein Update oder Upgrade auch vorenthalten.

Grundsätzlich besteht MU 6.0 aus zwei Komponenten: Der Service-Infrastruktur, die die MU Dienstleistung über das Internet anbietet, d.h. die “MU Service Site”, und dem “Update Client” auf dem Rechner des Nutzers, der diese Dienstleistung in Anspruch nimmt.

Mit WSUS2.0 ist es möglich, seinen eigenen Update Server zu betreiben. Nutzer, die Updates nur nach speziellen Tests zur Verfügung stellen wollen oder die keinen direkten Online-Zugriff auf den Arbeitsplatzrechner herstellen können oder wollen, können diese Komponente als Erweiterung eines Windows-Servers mit Online-Zugang installieren. WSUS2.0 wird dann die von Microsoft zur Verfügung gestellten Updates spiegeln. Im Ergebnis können die jeweiligen Entscheidungsgremien juristischer Personen des privaten oder öffentlichen Rechts selbst bestimmen, ob ein Update überhaupt angeboten wird und welche Updates für welche Arbeitsplatzrechner angeboten werden. Bezüglich des Designs stellt sich die WSUS-Corporate-Instance wie eine Kopie des MU Service dar: Das Protokoll ist so konstruiert, dass es mit einem einzigen einheitlichen Design zur Verfügung gestellt wird, das sowohl für die Verbindung Client/Corporate Server als auch für die Verbindung Client/Microsoft Update Service Communications optimiert ist. Aus Sicht des Rechners des Nutzers ist die Schnittstelle der WSUS-Corporate-Instance fast identisch mit der der MU Service Seite.

Die Ergebnisse der Datenschutzprüfung gelten nur für Microsoft Update Service 6.0 (MU 6.0) und Microsoft Windows Server Update Service 2.0 (WSUS 2.0). Die Produkte dürfen nur in folgenden Netzwerkumgebungen benutzt werden:

MU 6.0 Client:
Betriebssysteme: Windows XP Home Edition SP2, Windows XP Professional SP2
Internet Explorer 6.0 oder höher

WSUS 2.0
Betriebssysteme: Windows 2000 Server SP4, Windows 2003 Server

Nutzer von MU 6.0 und Administratoren von WSUS 2.0 müssen sicherstellen, dass Nutzerrechner und -server mit Hilfe von Virenschutzanwendungen und Firewalls ausreichend gegen feindliche, kodierte oder direkte Angriffe auf die Datenschutzfunktionen des ToE geschützt sind.

Von der zu untersuchenden Dienstleistung sind die folgenden Dienstleistungen und Funktionen nicht umfasst:

Produktaktivierung /-registrierung, Feedback- (Responses-) procedure, Survey-procedure, Windows Genuine Advantage (WGA), Piracy Report, CD-Order.

Werkzeuge, die für die Herstellung des IT-Produktes verwendet wurden

- 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

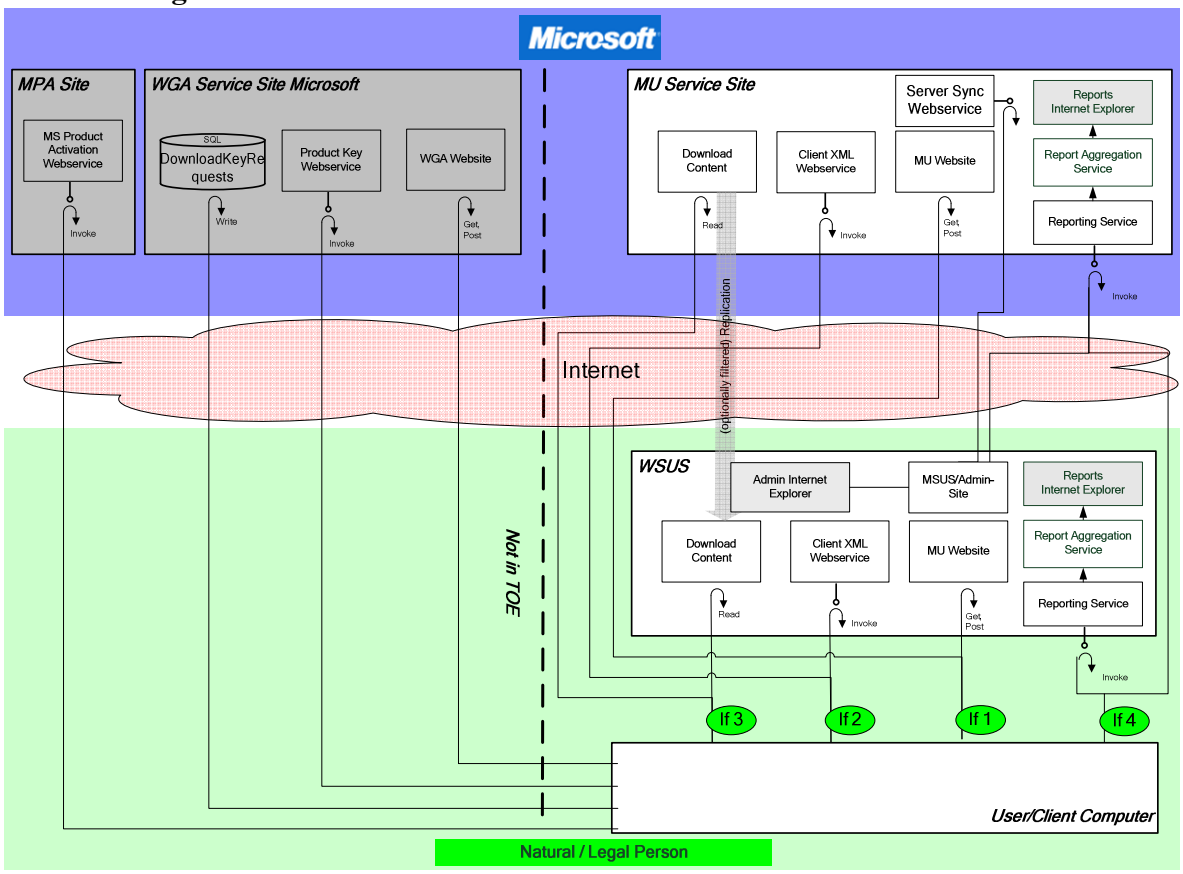
Zweck und Einsatzbereich

Insbesondere im Hinblick auf Angriffe, die aus Programmierfehlern resultieren, wie z.B. der Überlauf des Puffers, ist das Aufspielen sowohl von spezieller Update- als auch Upgrade-Software (z.B. Sicherheitsupdates, andere Updates und Verbesserungsupdates) unerlässlich für das ordnungsgemäße Funktionieren einer Datenverarbeitungsinstallation. Daher ist der Sinn des ToE der Erhalt und die permanente Verbesserung der ordnungsgemäßen Funktion der Datenverarbeitungsinstallation und dadurch die Unterstützung der IT-Sicherheit und der Datenschutzstrategie des Nutzers. Das ToE kann sowohl innerhalb von nicht-öffentlichen (geschäftlich und privat), wie auch innerhalb von öffentlichen Datenverarbeitungsinstallationen angewendet werden, vorausgesetzt, das folgende Umfeld ist gegeben:

MU 6.0 client:
Betriebssysteme: Windows XP Home Edition SP2, Windows XP Professional SP2
Internet Explorer 6.0 und darüber

WSUS 2.0
Betriebssysteme:
Windows 2000 Server SP4, Windows 2003 Server

Modellierung des Datenflusses



Ein Nutzer erhält Microsoft Updates entweder direkt von der MU Service Seite oder indirekt von einer zwischengeschalteten WSUS – Instanz. Der Client-Rechner verbindet sich entweder über das Internet mit der MU Service Seite oder über das Organisationsnetzwerk mit dem WSUS-Server. Der WSUS-Server erhält dabei die verfügbaren Updates von der MU Service Seite über das Internet, und ein IT-Administrator verwaltet die Verteilung von Updates von dem WSUS-Server auf die Client-Rechner.

Version des Anforderungskatalogs, die der Prüfung zugrunde gelegt wurde

Version 1.2

Zusammenfassung der Prüfungsergebnisse

TÜV Informationstechnik GmbH (TÜViT), Unternehmensgruppe TÜV NORD – und 2B Secure – die akkreditierte Prüfstelle für Datenschutz der 2B Advice GmbH – überprüften im Auftrag der Microsoft Inc., Redmond, Microsoft Update Service 6.0 (MU6.0) und Windows Server Update Service (WSUS 2.0) von April 2005 bis November 2006. Es wurde zunächst eine rechtliche Prüfung der Erklärungen, Policies und Spezifikationen durchgeführt, um die Anforderungen der technischen Prüfung festzulegen. Im Ergebnis tragen die Datenbank, die dem Programm zugrunde liegt, sowie der Quellcode und seine Anwendungen den Datenschutzanliegen Rechnung. Die Prüfung wurde auf der Grundlage von Dokumenten, Erklärungen und teilweiser Quellcodeinspektion durchgeführt. Microsoft hat die Safe-Harbor-Vereinbarung über Mitarbeiter- und Kundendaten am 29. Juni 2001 unterzeichnet.

Die Prüfung ergab, dass es fraglich ist, ob man von der zu untersuchenden Dienstleistung überhaupt sagen kann, sie erhebe, verarbeite oder speichere personenbezogene Daten. Die einzige Situation innerhalb der zu untersuchenden Dienstleistung, in der möglicherweise personenbezogene Daten erhoben und verarbeitet werden, ist die Nutzung von WSUS 2.0. Dort könnte ein WSUS-Administrator möglicherweise „Report-System"-Daten eines bestimmten Rechners, z.B. Daten, die den Update-Status, den Computer-Status oder die Synchronisierung der WSUS-Einstellungen betreffen, mit Hilfe des Security Identifier (SID), der Zeichenfolge "UserAccountName" und anderen Domain-Account-Daten, zu denen ein WSUS-Administrator gewöhnlich Zugang hat, mit einem bestimmten Mitarbeiter innerhalb einer Organisation in Verbindung bringen.

Selbst wenn man der Auffassung folgt, dass im Rahmen von Microsoft Update 6.0 (MU 6.0) aus Sicht von Microsoft IP-Adresse oder PID als personenbezogene Daten anzusehen sind, so dürfte deren Erhebung, Verarbeitung, Nutzung und Speicherung von einer gesetzlichen Grundlage gedeckt sein. Die Erhebung sowohl von IP-Adresse und PID erfolgt zu einem legitimen Zweck, und die erwähnten Datentypen werden unverzüglich wieder gelöscht. Das ToE muß Informationen einzelner Rechner, die das zu untersuchende IT-Produkt nutzen, ermitteln und aufzeichnen, um überprüfen zu können, ob Updates benötigt werden, und ob das Herunterladen und die Installation der einzelnen Updates erfolgreich waren. Deshalb ist der Zweck der Erhebung, Verarbeitung, Nutzung und Speicherung sowohl der IP-Adresse als auch der PID das reibungslose Funktionieren und die Sicherheit der Datenverarbeitungsinstallation von Nutzern von Microsoft-Produkten. Im Hinblick auf die Nutzerseite hält Microsoft die Protokolle 7 Tage lang auf dem IIS-Server und 30 Tage lang auf Band gespeichert. Microsoft protokolliert nicht die Bezugsadresse („Referrer Address"). Im Hinblick auf den "Reporting Service" werden IP-Adressinformationen nicht länger als 3-4 Stunden vorgehalten. Sobald Microsoft Daten zu einer bestimmten Stunde verarbeitet hat, werden alle Informationen zu IP-Adressen verworfen.

Im Fall von WSUS ist es ebenfalls fraglich, ob die vorgenannten „Report-System-Daten" eines bestimmten Rechners personenbezogene Daten im Sinne von § 3 Abs. 1 BDSG und § 2 Abs. 1 LDSG-SH darstellen. Selbst wenn man dies annimmt, so ist deren Erhebung, Nutzung und Verarbeitung von den gesetzlichen Erlaubnistatbeständen gedeckt. Letztendlich obliegt es dem WSUS-Administrator, Prozesse so zu gestalten, dass sie den jeweiligen Datenschutzanforderungen genügen.

Im Hinblick auf Mitarbeiter der öffentlichen Verwaltung und Beamte wird die Erhebung, Verarbeitung, Nutzung und Speicherung vorgenannter Daten auf die Erlaubnisnormen § 13 Abs. 1 BDSG und § 14 Abs. 1 BDSG in Verbindung mit § 14 Abs. 4 BDSG, bzw. entsprechender landesgesetzlicher Vorschriften, wie z.B. § 11 Abs. 1 LDSG-SH und § 13 Abs. 2 LDSG-SH in

Verbindung mit § 13 Abs. 6 LDSG-SH gestützt werden. Im Hinblick auf Mitarbeiter nicht-öffentlicher Stellen beruhen die Erhebung, Verarbeitung, Nutzung und Speicherung vorgenannter personenbezogener Daten auf der Erlaubnis nach § 28 Abs. 1, Satz 1 Nr. 2 BDSG in Verbindung mit § 31 BDSG.

Das "Microsoft Update Privacy Statement" erfüllt in Bezug auf die Unterrichtungspflicht gerade noch die Anforderungen des § 4 Abs. 1 TDDSG. Es besteht jedoch noch Raum für Verbesserungen. Im Hinblick auf Transparenz und Produktbeschreibung werden alle Betriebsanleitungen und Erklärungen zu den disponiblen Optionen aufgrund der Texte auf der Website klar und verständlich vermittelt. Bezüglich des "Microsoft Update Privacy Statement" wird jedoch dem Nutzer nicht hinreichend dargelegt, dass ein Cookie auf seinem Rechner abgelegt wird, wie lange dieses Cookie auf dem Rechner bleiben wird, und wie der Nutzer das Cookie wieder löschen kann. Außerdem ist es notwendig, dass Microsoft darüber unterrichtet, dass Daten in den Vereinigten Staaten von Amerika genutzt und gespeichert werden sowie dass weitere Erläuterungen gegeben werden, z.B. im Form von Definitionen und Beispielen, weil der Nutzer bestimmte Begriffe, wie z.B. "GUID" oder "PID", auf Anhieb nicht verstehen dürfte. Microsoft hat erklärt, dass das Unternehmen bereits begonnen hat, die obigen Belange in einer überarbeiteten Version des "Microsoft Update Privacy Statement" und des "Windows Update Privacy Statement" zu berücksichtigen. Ein neues „Microsoft Update Statement" wird nach Angaben von Microsoft spätestens Ende März 2007 veröffentlicht werden.

Aus Sicht eines lokalen Administrators, der MU6.0 mit WSUS2.0 implementiert und einrichtet, sind die Anleitungen auf den jeweiligen Webseiten und die WSUS-Online-Hilfe geeignet, einen Administrator bei den jeweiligen Administrationsaufgaben zu unterstützen.

Darüberhinaus sind im Hinblick auf § 4 Abs. 4 TDDSG und § 9 BDSG inklusive des Annexes zu § 9 Satz 1 BDSG technische und organisatorische Maßnahmen implementiert, die sicherstellen, dass keine Kombination von Nutzungsdaten verschiedener Microsoft Online-Dienste erfolgt: Microsoft hat den Dienst des ToE als „Dedizierten Microsoft Online-Service" auf dedizierten Servern installiert.

Das ToE genügt schließlich auch den Anforderungen der Grundsätze von Datenvermeidung und Datenwirtschaftlichkeit nach § 4 LDSG-SH. Im Hinblick auf die Revisionssicherheit liegen zwar keine zusätzlichen technischen Vorkehrungen vor. Das Maß der Erforderlichkeit von Vorkehrungen zur Revisionssicherheit hängt jedoch vom jeweiligen Missbrauchspotential ab, welches für den vorliegenden Fall angesichts der begrenzten Möglichkeiten eines WSUS-Administrators auf der einen Seite und der Qualität der Daten auf der anderen Seite als verhältnismäßig niedrig zu bewerten ist. Es ist zudem zu beachten, dass Revisionssicherheit durch organisatorische Maßnahmen, wie z.B. dem Ausdruck von Berichten, sichergestellt werden kann.

Beschreibung, wie das IT-Produkt Datenschutz und –sicherheit unterstützt

Das ToE stellt folgende Funktionen zur Verfügung, die Datenschutz und -sicherheit unterstützen:

- Nutzerfreundliche Bereitstellung wichtiger Updates gegen ständig neue Sicherheits- und Datenschutzgefahren
- Systemeinstellungen mit Terminierungs- und Benachrichtigungsoptionen
- Schutz der Integrität von Update-Dateien durch elektronische Signaturen und Signaturverifizierung
- Updates für Endnutzer und geschäftliche WSUS-Instanzen

WSUS 2.0 sieht Folgendes vor:

- Funktionen zum Verwalten und Weiterleiten von Updates durch Administratoren
- Updates für verschiedene Microsoft Betriebssysteme und Produkte
- Automatischer Download von Updates je nach Produkt, Typ und Sprache
- Anpassung von Updates an spezielle Zielrechner und Rechnergruppen
- Überprüfung der Tauglichkeit von Updates vor Installierung
- Berichts- und Auswertungsmöglichkeiten
- Flexible Skalierbarkeit für eine große Bandbreite an Organisationen

MU6.0 und WSUS 2.0 entsprechen dem derzeitig möglichen technischen Stand. Updates, Upgrades und zusätzliche Gratis-Software werden für den Nutzer von Microsoft Produkten zur Verfügung gestellt, ohne dass nicht erforderlich personenbeziehbare Daten verarbeitet werden.
Die Fähigkeit von MU6.0 und WSUS 2.0 zur Verbesserung des Datenschutzes hängt von den Bedingungen der eingesetzten IT-Umgebung ab.
Die Nutzer und Administratoren von MU 6.0 und WSUS 2.0 sollten sicherstellen, dass sowohl Client als auch Server ausreichend durch Virenscanner und Firewalls gegen schädlichen Code oder feindliche Angriffe auf die den Datenschutz und die Datensicherheit unterstützenden Funktionen des ToE geschützt sind. Darüberhinaus sollte der WSUS-Server innerhalb der Firewall einer Organisation installiert werden.