Datenschutzaudit

Kurzgutachten Version 1.0g

für die Verleihung des

ULD Datenschutz-Gütesiegels

-Final-

Objekt der Bewertung (ToE)

Microsoft Software Protection Platform

Stand: 01.11.2008

1

Kurzgutachten

2 Name und Version des IT-Produkts:

Microsoft Software Protection Platform (SPP)

Stand 01.11.2008

3 Hersteller des IT Produkts:

Microsoft Corporation

One Microsoft Way

Redmond, WA 98052-6399

USA

4 Zeitraum der Prüfung:

Juni 2007 bis November 2008

5 ULD Experten, die das IT-Produkt geprüft haben:

Prüfstelle für Datenschutz (rechtlich)

2B Advice GmbH

Marcus Belke, Rechtsanwalt

Wilhelmstrasse 40-42

53111 Bonn

Deutschland

marcus.belke@2b-advice.com

Prüfstelle für Datenschutz (Technisch)

TÜV Informationstechnik GmbH

Stephan Di Nunzio

Langemarckstrasse 20

45141 Essen

Germany

S.DiNunzio@tuvit.de

6 Zertifizierungsstelle:

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Holstenstr. 98

D-24103 Kiel

Deutschland

7 Spezifikationen des Objekts der Bewertung (ToE):

Microsoft Software Protection Platform ist der Name für die Zusammenfassung der Dienste Activation, Volume License Management und Security Breach Response. Die Ergebnisse der Datenschutzprüfung sind ausschließlich auf die Microsoft Software Protection Platform anwendbar.

Das Produkt muss in der folgenden Umgebung eingesetzt werden: Betriebssysteme: Windows Vista RTM sowie Windows Vista SP1, Windows Server 2008 RTM.

RTM ist die Abkürzung für "Release to Manufacture" und beschreibt die erste veröffentlichte Version von Vista und Windows Server 2008.

Die Hauptanwendungsszenarien der Software Protection Platform sind:

Einzellizenzaktivierung

Aktivierung durch Originalhersteller (OEM)

Volumenlizenzaktivierung mit Key Management Server (KMS)

Volumenlizenzaktivierung mit Volume License Activation Management Tool (VAMT)

Windows Genuine Advantage (WGA)

Breach Response Tool (BRT)

Der Echtheitstest im Allgemeinen sowie der Update-Mechanismus sind nicht Teil des ToE. Die WGA 1.7 und MU 6.0 Komponenten wurden für Windows XP in einem früheren Datenschutzsiegelverfahren bereits geprüft.[1] Es wird lediglich die Datenübertragung zwischen der Software Protection Platform und diesen Komponenten in dieser Prüfung begutachtet.

8 Allgemeine Beschreibung des Produktes

Bei der Microsoft Software Protection Platform handelt es sich um einen Dienst, der Mechanismen für Kunden und Organisationen bereitstellt, die sie vor dem Risiko von Softwarefälschungen schützen und Kunden von Volumenlizenzen eine bessere Verwaltung ihres Softwarebesitzes ermöglichen. Das Gesamtziel der Software Protection Platform ist die Zusammenführung von neuen Anti-Piraterie-Innovationen, Fälschungserkennungsverfahren und Resistenz gegen Manipulationen. Die Kombination dieser Verfahren in einer vollständigen Plattform bietet einen größeren Softwareschutz für Programme, die die Software Protection Platform nutzen. In der ersten Stufe wird die Software Protection Platform nur von Microsoft Windows Vista und Microsoft Windows Server 2008 genutzt, um die Systeme vor Softwarepiraterie zu schützen. Der Hauptvorteil der Software Protection Platform besteht darin, dass in allen Kommunikationsschritten kryptographische Verfahren genutzt werden, um die Integrität der Kommunikation wie auch der Systeme zu schützen.

Die Software Protection Platform bietet zwei Hauptzugangspunkte. Der erste Zugang zur Software Protection Platform ist die Softwareaktivierung, die jedes Produkt mindestens einmal durchzuführen hat. Bevor ein Microsoft-Betriebssystem, das die Software Protection Platform nutzt, vollumfänglich genutzt werden kann, muss es aktiviert werden. Der zweite Zugangspunkt zur Software Protection Platform ist die Absicherung des Echtheitsstatus der Software innerhalb des Downloads von speziell geschützter Software von Microsoft. Der Echtheitstest ist erforderlich, um auf das Microsoft Download Center oder Windows Update zuzugreifen. Diese Windows Downloads und Updates werden nur für genuine Windowssysteme zur Verfügung stehen.

[1] https://www.datenschutzzentrum.de/guetesiegel/kurzgutachten/g070908/g070908-kurzgutachten-microsoft-wga-deutsch.pdf

9 Grenzüberschreitende Belange

Das Produkt Software Protection Platform wird weltweit angeboten und genutzt. Alle Daten werden in einem Microsoft Corporation Datencenter in den USA gespeichert.

10 Tools, die bei der Entwicklung des Produktes genutzt wurden

Microsoft Visual Studio .Net Professional 2003 & 2008
Microsoft Office Professional Edition 2003 & 2007
Microsoft Office Visio Professional 2003 & 2007
Microsoft Office Project Professional 2003 & 2007
Microsoft Product Studio 2.10.6729.0
Microsoft Source Depot 3.0
Microsoft FxCop 1.3
Microsoft SQL Server 2000
Warbird 1.1.10
Microsoft Prefast
Microsoft Prefix
Microsoft APTool
Microsoft SQL Server

11 Version des Anforderungskataloges

ULD Anforderungskatalog, Version 1.2 (29. August 2005)

12 Ergebnisse der Begutachtung

Die Begutachtung der Microsoft Software Protection Platform ergab als Gesamtergebnis, dass die Verarbeitung personenbezogener Daten in einer vorbildlichen Weise umgesetzt ist. Die verschiedenen Anwendungsszenarien wurden detailliert begutachtet:

1. Einzellizenzaktivierung
Grundsätzlich muss jedes Microsoft-Betriebssystem aktiviert werden. Systeme, die den Aktivierungsprozess nicht innerhalb einer Frist von 30 Tagen durchführen, werden in der RTM-Version in einen Modus reduzierter Funktionalität und in der SP1-Version in einen Benachrichtigungsmodus versetzt. Während im Modus reduzierter Funktionalität die Benutzung des Systems auf die grundlegenden Funktionen beschränkt ist, ist das System im

Benachrichtigungsmodus vollumfänglich nutzbar, es wird nur für eine kurze Zeit eine Nachricht eingeblendet, dass die Software noch nicht aktiviert ist.

Im Einzellizenzaktivierungsszenario kauft der Nutzer Windows Vista oder Windows Server 2008 in einem Geschäft und installiert es auf einem beliebigen Computersystem. In diesem Fall muss er das System entweder online oder telefonisch aktivieren. In einigen Ländern kann die Aktivierung alternativ auch über den Short Messaging Service (SMS) eines Handys durchgeführt werden. Im Online-Teil der Einzellizenzaktivierung wird eine Verbindung zwischen Microsoft und dem Client-PC des Nutzers aufgebaut. Microsoft installierte eine Kommunikationsschicht mit Namen Software Licensing Service. Diese Schicht innerhalb Microsofts verwaltet die Kommunikation mit dem Client-PC.

Microsofts zweite Schicht nach der Kommunikation ist die Datenbankschicht. Die Clientkommunikation wird durch die Kommunikationsschicht gefiltert und an die Datenbankschicht mit Namen Activation Service Clearinghouse weitergeleitet. Diese Schicht beinhaltet die Datenbanken, die zeitlich unbegrenzt gespeichert werden.

Die Begutachtung ergab, dass bei der Verbindung zu Microsoft keine personenbezogenen Daten übertragen werden. Als Gegenstand der Onlinekommunikation wird jedoch die IP-Adresse des Computers übertragen. Diese IP-Adresse wird nur solange genutzt und gespeichert, wie es notwendig ist, um die Anfrage des Clientgerätes zu beantworten.

Zusätzlich wird der Computername des Gerätes, den der Nutzer während der Installationsroutine eingeben kann, an die Kommunikationsschicht der Software Protection Platform übertragen. In der Kommunikationsschicht können Informationen zu Debuggingzwecken wenn nötig mitgeschnitten werden. Das Mitschneiden kann nur freigegeben werden, wenn ein vorher festgelegter Genehmigungsprozess durchlaufen wurde. Die Begutachtung ergab, dass in Fällen, in denen ein Nutzer seinem Computersystem einen echten Namen bezogen auf eine natürliche Person gibt, personenbezogene Daten an Microsoft übertragen werden könnten. Die Standardeinstellung für das Feld "Computername" ist der erste eingegebene Benutzername mit dem Appendix „-Computer". Der Prüfer rät Nutzern, keinen echten Personennamen in das Feld "Computername" einzugeben. Gibt der Nutzer einen echten Namen als Computernamen ein, werden personenbezogene Daten übertragen und möglicherweise von Microsoft gespeichert, bis die folgenden Änderungen umgesetzt wurden:

Nach einem Hinweis im Begutachtungsprozess entschied sich Microsoft, die Aufzeichnung von IP-Adresse und Computernamen zum 17.Oktober 2008 zu beenden. Die Übertragung des Computernamens wird mit einem Clientupdate am 19. Januar 2009 vollständig beendet. Wegen der Notwendigkeiten der TCP/IP- Kommunikation kann die Übertragung der IP-Adresse nicht vollständig verhindert werden, die Daten werden aber nur solange gespeichert, wie es zur Kommunikation notwendig ist.

Daneben werden einige für Microsoft nicht personenbezogene, aber eindeutige Daten wie Hard- und Softwareprüfsummen sowie der Product Key in vier Kommunikationsschritten an Microsoft übertragen. Die eindeutige Hardwareprüfsumme wird bezogen auf die Client-Hardware generiert. Diese Hardware-Information wird mit der endgültigen Lizenz verknüpft, welche die korrekte Nutzung ermöglicht. Der Wechsel zu vieler Hardwarekomponenten macht daher eine Reaktivierung erforderlich. Die Hardwareprüfsumme ist für Microsoft ein nicht personenbezogenes Datum. Während der Begutachtung ergaben sich für die Gutachter keine Zweifel an der Aussage von Microsoft, dass man keine Referenz zu den pseudonymen Daten hat. Die gleichen Überlegungen gelten für den Product Key, der ebenfalls eindeutig ist und von Microsoft verarbeitet wird. Der Product Key wird auch im WGA 1.7 Verfahren genutzt. Dort wurde geprüft, ob der Product Key zu einer Re-Personalisierung führen kann, da in den Fälschungsaustauschverfahren von WGA 1.7 Microsoft personenbezogene Daten (Adresse des Kunden, Adresse des Verkäufers des gefälschten Produktes) in Kombination mit dem Product Key der gefälschten Software erheben muss, um eine Ersatzkopie des Produktes zur Verfügung zu stellen. In allen Fällen des WGA 1.7 Fälschungsaustauschs ist der Product Key, der mit einer natürlichen Person kombiniert ist, ein gefälschter Key; er wird auch nicht länger genutzt, da der Kunde in diesem Prozess die gefälschten Medien an Microsoft schickt. In diesen Szenarien ist eine Aktivierung nicht länger möglich. Die Begutachtung hat gezeigt, dass keine Kombination von Unique Identifiern mit personenbezogenen Daten (wie Namen) innerhalb der Software Protection Platform möglich ist.

Die Einzellizenzaktivierung ist auch mit einer telefonischen Aktivierung möglich. In diesem Szenario generiert das Produkt einen annähernd eindeutigen Wert der Hardware, der von der Hotline verwendet wird, um einen Aktivierungscode zu generieren. Der Nutzer muss diesen Code in ein vorgefertigtes Formular eingeben. Die Kommunikationswege in diesem Szenario sind das Telefon und das Handy bzw. die SMS. In diesem Szenario werden weniger eindeutige Daten übertragen, da die Hardwareprüfsumme gekürzt wird. Die Problematik des Computernamens, der möglicherweise persönliche Informationen enthalten kann, tritt in

diesem Szenario nicht auf. Es gibt keine personenbezogenen oder zumindest pseudonyme Daten in der Telefon- oder Short Messaging Service Aktivierung.
Der Benutzerdatenschutz ist in der Online-Aktivierung und der Telefon-/SMS-Aktivierung angemessen umgesetzt.

2. OEM Aktivierung
Die von einem Originalhersteller durchgeführte Aktivierung erfolgt ohne personenbezogene Daten. Das System wird, bevor es an einen Nutzer verkauft wird, vollständig aktiviert. Es ist keine weitere Interaktion mit Microsoft erforderlich. Dies gilt nicht, wenn der Nutzer die Hardware über eine bestimmte Schwelle hinaus verändert oder er seinen Computer von Wiederherstellungsmedien reparieren muss. In diesen Fällen muss der Nutzer eine Einzelaktivierung durchführen. Der Benutzerdatenschutz ist im OEM Aktivierungs-Szenario hervorragend umgesetzt.

3. Volumenlizenzaktivierung mit Key Management Server (KMS)
Volumenlizenzen sind Produkte, die eine festgelegte Anzahl von Computern aktivieren können. Um Firmen und öffentliche Stellen bei der Aktivierung ihrer Computer zu unterstützen, hat Microsoft den Key Management Server (KMS) erfunden. Dieser KMS ist ein innerhalb der Firma oder der öffentlichen Stelle gehostetes System, das selbst online oder per Telefon aktiviert wird. Der KMS verwaltet die Aktivierung von Clients im internen Netzwerk. Clients oder andere interne Server aktivieren sich gegen den KMS, der die Lizenzen an die Geräte verteilt. Der KMS läuft nur in größeren Netzwerken mit mindestens 25 Clientgeräten oder 5 Servergeräten. Die von einem KMS aktivierten Geräte müssen sich innerhalb eines variablen Zeitraums reaktivieren. Administratoren des KMS können diesen festlegen. Die maximale Reaktivierungszeit beträgt 180 Tage.

Unter Berücksichtigung der Tatsache, dass keine Kommunikation interner Geräte mit Microsoft mit Ausnahme des ersten Gerätes, das den KMS hostet, stattfinden muss, sind die Auswirkungen auf den Nutzerdatenschutz minimal. Jedoch wird in der internen Kommunikation der vollständige Domainname eines Gerätes benutzt und in der KMS-Datenbank gespeichert. Dieser Domainname enthält auch den Computernamen, der auch hier wieder den Namen des Nutzers enthalten kann. An dieser Stelle wird Administratoren eines Netzwerkes geraten, nicht die Namen von natürlichen Personen für Geräte zu verwenden. Dies ist keine Datenschutzverletzung durch SPP, sondern liegt in der Verantwortung der Netzwerkadministration der Organisation, die den KMS einsetzt. Der Nutzer kann den

Computernamen an den folgenden Stellen überprüfen: „Computer / Systemeigenschaften“ und „Systemsteuerung / System“.
Der Benutzerdatenschutz ist im KMS Aktivierungsszenario hervorragend umgesetzt.

4. Volumenlizenzaktivierung mit Volume License Activation Management Tool (VAMT)
Für kleinere Einrichtungen oder Laborszenarien bietet Microsoft ein herunterladbares Programm namens Volume License Activation Management Tool (VAMT), das verschiedene einzelne Module zur Erfüllung der Anforderungen enthält. VAMT ist eine mobile Anwendung, die als Proxyserver betrieben werden kann, um Anfragen von Geräten, die nicht mit dem Internet verbunden sind, weiterzuleiten; außerdem kann sie als Sammler und Verteiler arbeiten, um eine Anzahl von Geräten in einem automatisierten Prozess sogar in vollständig offline befindlichen Laboratorien oder Hochsicherheitsszenarien zu aktivieren. Der VAMT Proxy leitet die Anfragen direkt an Microsofts SPP-Server weiter. Außer dem Computernamen, der nicht übertragen wird, werden die Unique Identifier wie im Onlineaktivierungsszenario an Microsoft weitergeleitet. In diesem Szenario stammt die IP-Adresse, die an Microsofts Kommunikationsschicht eintrifft, von dem VAMT-Proxy-Gerät und nicht vom Clientgerät.
Der Benutzerdatenschutz ist im VAMT Activation Szenario hervorragend umgesetzt.

5. Windows Genuine Advantage (WGA)
Bei Windows Genuine Advantage handelt es sich um ein Modul von Microsoft, um das System gegen betrügerische Nutzung zu schützen. Windows Genuine Advantage 1.7 für Windows XP ist nicht Teil dieser Begutachtung. Es wurde früher bereits begutachtet. Trotzdem gibt es einen Informationsaustausch zwischen SPP und WGA 1.7. Dieser Austausch wurde innerhalb dieser Begutachtung geprüft. Eine WGA-Prüfung ist notwendig, um spezielle Inhalte aus dem Microsoft Download Center herunterzuladen. Nur echten Systemen wird der Vorteil gewährt, spezielle Inhalte aus dem Download Center zu erhalten. Im SPP Szenario wird eine Lizenzanfrage an das SPP-Modul verschickt. Dieses SPP-interne Modul prüft die Unversehrtheit des Systems und den Aktivierungsstatus in der Aktivierungsdatenbank. Wenn die Prüfung positiv ausfällt, wird eine temporäre WGA-Lizenz erteilt. Bei dieser Lizenz handelt es sich um eine kryptographische Lizenz mit der Erlaubnis, spezielle Inhalte aus dem Microsoft Download Center herunterzuladen. Die Lizenz selbst enthält keine Information über den Clientcomputer. Die Kommunikation innerhalb SPP, um eine Lizenz zu erhalten, erfolgt als interner Austausch von Modulinformationen, die bereits vorher erhoben wurden. Es werden keine neuen Informationen während dieses Verfahrens übertragen.

Dies ist ein hervorragender Weg, die Unversehrtheit eines Systems zu prüfen, ohne dabei auch nur intern Geräteinformationen einzuschließen.

6. Breach Response Tool (BRT)

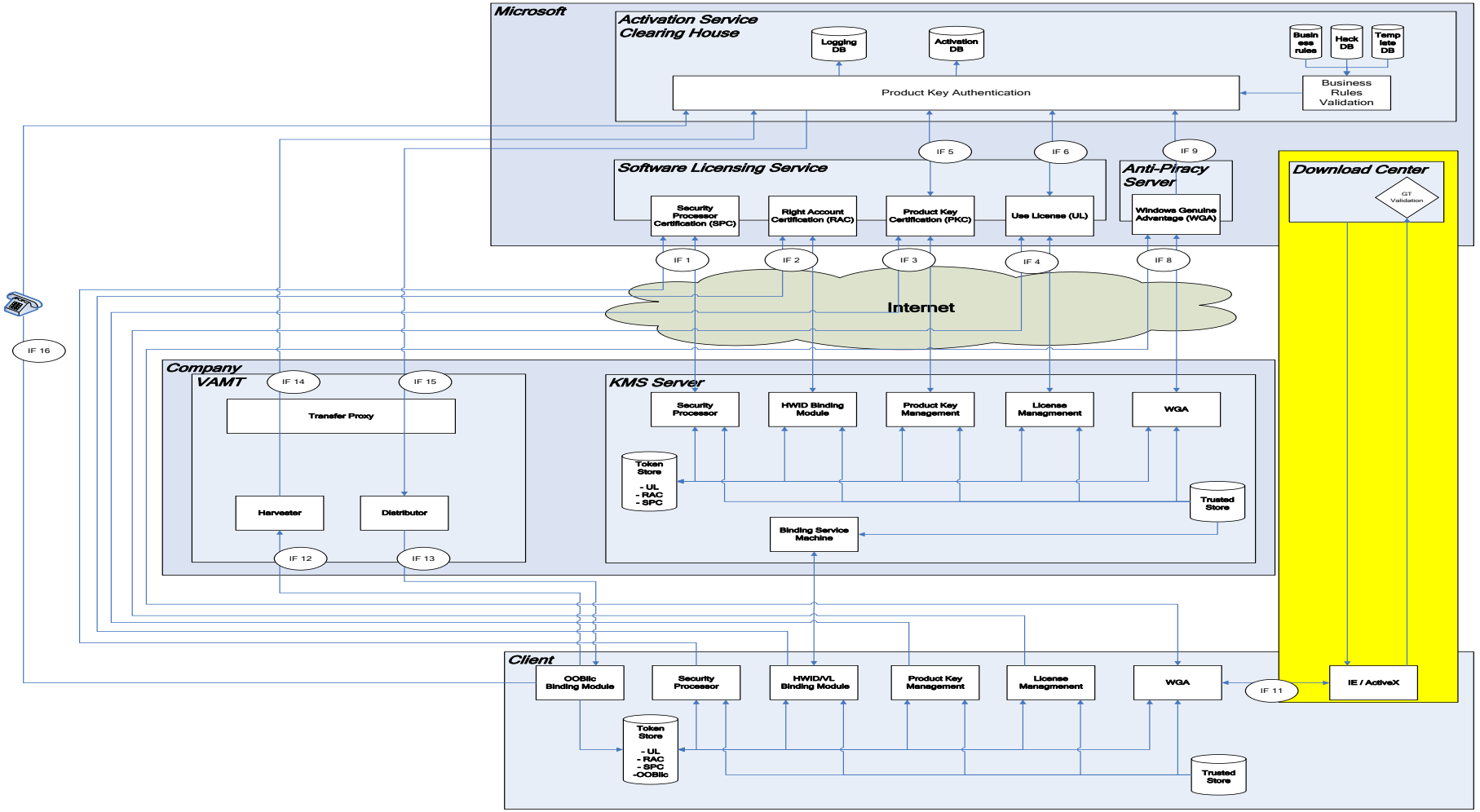
Das Breach Response Tool dient der Abwehr von Verletzungen des Sicherheitssystems von SPP. SPP wurde - wie andere Produkte auch - so entworfen, dass es sich gegen alle Manipulationen verteidigt, deren Ziel es ist, die Notwendigkeit einer Produktaktivierung zu umgehen. Softwarepiraten gelang es, Exploits zu entwickeln, die es ermöglichten, das Betriebssystem ohne Aktivierung zu nutzen. Diese Exploits bergen die Gefahr von verseuchten, instabilen Systemen. Um den Nutzer vor diesen instabilen Systemen zu schützen, prüft das BRT das System gegen bekannte Exploits. Das BRT wird über den Windows Update Mechanismus verteilt und ausgelöst. In der Standardeinstellung ist der Update Service abgeschaltet und startet nicht automatisch. Der Nutzer hat die Möglichkeit das BRT Update nicht zu installieren. Falls sich der Nutzer dazu entscheidet, den Update Service zu starten, wird er informiert, dass Informationen an Microsoft gesendet werden können. Dieselbe Information wird angezeigt, wenn sich der Nutzer zum Wechsel zu automatischen Updates entscheidet. Zusätzliche Informationen werden auf der Webseite angeboten, die vom Update Service aus erreicht werden kann. Entscheidet sich der Nutzer zu einem beliebigen Zeitpunkt für die automatische Installation von Updates, wird er informiert, dass alle Updates ohne weitere Information installiert werden.

Der Nutzer kann zusätzliche Informationen zu BRT Update erhalten, wenn er dem Link zu der zugehörigen Webseite folgt. Normalerweise erwartet der Microsoftnutzer Informationen zur Datenverarbeitung in der Datenschutzerklärung. Nach einem Hinweis durch die Gutachter, hat sich Microsoft dazu entschieden, eine Link von der BRT Informationsseite zu der zugehörigen Datenschutzerklärung (http://www.microsoft.com/genuine/downloads/PrivacyInfo.aspx) einzufügen. In der Datenschutzerklärung sind zusätzliche Informationen zu der Datenübermittlung von BRT aufgeführt. Es wird dargestellt, dass auch dann Daten von Windows Vista SP 1 gesendet werden, wenn keine Manipulation vorliegt.

Im RTM-Modus von Windows Vista werden Informationen nur gesendet, wenn eine Verletzung gefunden wurde. Vista SP1 sendet immer Informationen an Microsoft, sogar wenn das System nicht manipuliert ist. Nur in Volumenlizenzszenarien kann diese Telemetrie abgeschaltet werden. Die übertragenen Informationen sind vollständig für Microsoft nicht personenbezogen und werden für statistische Zwecke genutzt.

Mit Blick darauf, dass die erhobenen Daten nicht personenbezogen sind, gibt es keine wesentlichen Auswirkungen auf den Benutzerdatenschutz.

13 Datenflussmodell



14 Wie das Produkt den Datenschutz verbessert:

Die Software Protection Platform verbessert den Datenschutz, indem sie Millionen von Nutzern die Möglichkeit bietet

- den Aktivierungsstatus des Betriebssystems zu bestätigen und für Vista-Kunden von Einzelhandels- oder Volumenlizenzen eine rechtmäßige Softwareaktivierung des Betriebssystems sicherzustellen,
- den Nutzer zu warnen und illegale Aktivierungstools abzuschalten, die auf ihr Vista Betriebssystem angewandt wurden und
- den Nutzern die Möglichkeit zu bieten, ein genuines Betriebssystem zu erhalten, ohne datenschutzrelevante Daten zu sammeln.

All dies wird durch die Nutzung intelligenter Technologien anstelle der Sammlung personenbezogener Daten des Nutzers erreicht. Dies ist eine führende Technologie im Bereich der datenschutzfreundlichen Softwareaktivierung und des Urheberschutzes.

Das Zusammenspiel der lokalen ToE-Komponenten und der Software Protection Platform Dienste nutzt nur pseudonyme, anonyme und nicht personenbezogene Daten.

Auf diesem Weg respektiert Microsoft – als der Begründer der Software Protection Platform und Anbieter damit verbundener Dienste – die Privatsphäre der Nutzer des Betriebssystems Windows Vista und hilft den Nutzern, illegale Aktivierungstools zu entfernen, die vorher installiert wurden und das inhärente Risiko von Datenschutzverletzungen solcher Nutzerdaten beinhalten, die auf unrechtmäßig aktivierten Betriebssystemen verarbeitet werden.

15 Belange, die besondere Aufmerksamkeit des Nutzers erfordern:

Die Begutachtung hat gezeigt, dass im Installationsprozess die Standardeinstellung für den Computernamen der erste angelegte Benutzername mit dem Appendix "-Computer" ist. Im Hinblick auf Datenschutzbedenken raten wir dem Nutzer, den Computernamen auf einen nicht-personenbezogenen Namen umzustellen. Microsoft hat den Speicherprozess geändert, um dieses mögliche personenbezogene Datum aus allen Datenbanken herauszunehmen. Am 19. Januar 2009 wird ein Update zur Verfügung gestellt, das ausschließt, dass der Computernamen von der Clientsite übertragen wird.

Ein zweiter datenschutzrelevanter Hinweis betrifft das sog. Breach Response Tool, das als "Wichtiges Update" (KB940510) eingespielt und von Microsoft Update gestartet wird. Dieser Mechanismus prüft den Systemstatus. In Vista RTM wird keine Telemetrie an Microsoft gesendet, in Vista SP1 wird jedoch Telemetrie übertragen, selbst wenn das System nicht manipuliert worden ist. Es muss aber darauf hingewiesen werden, dass in der Telemetrie nur nicht personenbezogene Daten gesendet werden. Die Übermittlung der Telemetrie kann nur in Volumenlizenzszenarien abgeschaltet werden.

16 Ausgleich von Schwächen:

Es gibt keine Datenschutzschwächen in SPP, die ausgeglichen werden müssten.

17 Entscheidungstabelle mit relevanten Anforderungen:

Datenschutzprüfungs-anforderung	Entscheidung	Bemerkungen
Datenvermeidung und -minimierung	vorbildlich	Das SPP nutzt die IP Adresse zum Zwecke der Kommunikation. Daneben nutzt SPP keine personenbezogenen Daten. Die Aktivierung erfolgt auf Basis einiger weniger, nicht personenbezogener System Identifiers. Sogar der BRT-Mechanismus nutzt nur System Identifier, um den Systemstatus zu ermitteln und zu berichten.
Transparenz	adäquat	Microsoft bietet gut strukturierte Datenschutzinformationen. Diese Informationen sind in einer einfach zu verstehenden Art und Weise abgefasst.

Technisch-organisatorische Maßnahmen	vorbildlich	Die von Microsoft eingesetzten technischen und organisatorischen Maßnahmen sind beispielhaft. Microsoft hat einen Aktivierungsmechanismus erfunden, der auf kryptographischen Zertifikaten basiert.
Betroffenenrechte	nicht anwendbar	Allgemein werden keine personenbezogenen Daten an Microsoft übermittelt, so dass Microsoft auch keine speziellen Betroffenenrechte gewähren muss.

18 Zusammenfassung der Ergebnisse der Begutachtung:

Sowohl die rechtliche als auch die technische Begutachtung haben gezeigt, dass die Software Protection Platform die Softwareproduktaktivierung in einer datenschutzfreundlichen Art und Weise implementiert. Die Aktivierung erfolgt ohne die Speicherung personenbezogener Daten. Innerhalb des Aktivierungsprozesses wird ein eindeutiges Zertifikat generiert, welches das Betriebssystem aktiviert. Dieses Zertifikat enthält die verschlüsselte und signierte Antwort des Microsoft Activation Service. Derselbe datenschutzfreundliche Mechanismus wird genutzt, um den WGA-Test auf dem System auszuführen.

In Volumenlizenzaktivierungsszenarien kann die Privatsphäre durch den Einsatz von firmeninternen Aktivierungsservern geschützt werden. In diesen Fällen muss nur das Gerät, das den Server enthält, gegen Microsoft aktiviert werden. Alle anderen firmeninternen Geräte aktivieren sich gegen den firmeninternen Aktivierungsserver. In diesen Szenarien findet keine weitere Übermittlung an Microsoft statt.

Die Kommunikation zwischen SPP und WGA, um eine WGA-Lizenz zu gewähren, ist ebenfalls datenschutzfreundlich umgesetzt. Es werden keine personenbezogenen Daten oder sogar Unique Identifier, die eine Repersonalisierung ermöglichen könnten, zwischen den zwei Diensten innerhalb von Microsoft übertragen. Das WGA-Modul in SPP erzeugt und signiert eine Downloadlizenz, die an den WGA-Dienst übermittelt wird. Diese Lizenz ist zeitlich begrenzt, enthält jedoch keine Identifizierungsmerkmale, die personenbezogene Informationen einschließen.

Das letzte begutachtete Szenario, das Breach Response Tool, wurde wegen einiger Verletzungen des Sicherheitssystems in SPP implementiert. Bei Nutzung eines Exploits, der die Microsoft-Sicherheitsmechanismen abschaltet, besteht das Risiko von unerwarteten Abstürzen des Betriebssystems und Datenschutzverletzungen von Nutzerdaten. BRT wird nur im Windows Update Prozess ausgeführt. Nutzer, die keine Updates ausführen, erhalten BRT nicht. Wenn BRT einen Exploit auf dem System des Nutzers findet, führt es den Nutzer zurück zu einem stabilen Systemstatus. In der Version Vista SP1 sendet BRT Telemetrie an Microsoft. Es werden jedoch keine personenbezogenen Daten gesendet.

Als Gesamtbeurteilung ist festzustellen, dass SPP ein effizientes Lizenzschutztool ist, das Microsoftsoftware hinlänglich vor Manipulation und daher auch Nutzer von mit SPP ausgestatteter Microsoftsoftware vor Datenschutzverletzungen schützt.