Spinoniert Windows XP?

Spioniert Windows XP?

Datenübermittlung bei der Aktivierung und beim Update von Software

Moderne Software wird elektronisch verteilt, aktiviert, erneuert und gewartet. In Zusammenhang mit dem neuen Betriebssystem Windows XP wird Microsoft immer wieder vorgeworfen, die Internet-Verbindungen nicht nur für die Aktivierung, Erneuerung und Verbesserung der installierten Software, sondern auch zum Sammeln von Informationen über den Benutzer und dessen Systemkonfigurationen zu verwenden. Um diese Vorwürfe besser einordnen zu können, wurde am Institut für Internet-Technologien und -Anwendungen der Hochschule Rapperswil (ITA-HSR) untersucht, welche Daten Windows XP bei der Aktivierung und beim Update wirklich über das Internet an Microsoft sendet.

Peter Heinzmann, Marcel Liebi

Mit den neuen Anschlusstechniken ADSL und Cable Modem sind private Rechner dauernd mit dem Internet verbunden. Dies bietet den Software-Herstellern neue Möglichkeiten zur Installation, Überwachung und Fehlerbehebung. Am ITA-HSR wurden die Abläufe und die Art der über die Kundenrechner zu anderen Stellen geschickten Daten bei Software-Aktivierung, Registrierung, Aktualisierung und Error-Reporting analysiert.

Windows XP arbeitet mit so genannter *Software-Aktivierung*: Wer Windows XP länger als 30 Tage nutzen will, muss diese Software nicht nur kaufen, sondern nach ihrer Installation auch Microsoft kontaktieren, um einen Aktivierungs-Code zu erhalten. Die Software-Aktivierung kann über Internet oder Telefon erfolgen. So kann überprüft werden, ob das Produkt kopiert wurde; damit soll verhindert werden, dass Raubkopien zum Einsatz kommen.

Wie bei den meisten Software-Produkten gibt es auch bei Windows XP die Möglichkeit zur *Software-Registrierung*, bei welcher – via Internet oder auf dem Korrespondenzweg – der Software-Firma bekannt gegeben wird, welche Person ein bestimmtes Produkt gekauft hat. Die Firma kennt damit für jedes registrierte Produkt die Personendaten der Besitzer (Name, Adresse, evtl. auch Kaufdatum und Kaufort) und die eindeutige Seriennummer des entsprechenden Produktes.

Windows XP unterstützt ferner so genannte *Software-Aktualisierung*. Hier geht es darum, bereits installierte Software-Produkte via Internet auf den neusten Stand zu bringen, d.h. Updates anzufordern und zu installieren. Windows XP verwendet diesen Aktualisierungsprozess für das Betriebssystem und für verschiedenste Anwendungsprogramme.

Schliesslich bietet Windows XP auch die Möglichkeit zur *Übermittlung von Software-Fehlermeldungen* – «Error Reports» –, mit welchen Microsoft über Fehlfunktionen von Programmen informiert werden kann. Basierend auf solchen Reports will Microsoft die Zuverlässigkeit der Software verbessern.

Im vorliegenden Beitrag wird aufgezeigt, wie die verschiedenen Kommunikationsprozesse ablaufen, welche Daten bei der Software-Aktivierung und -Aktualisierung (Updates) sowie beim Error Reporting von Windows XP und Office XP an Microsoft geschickt werden und welches die kritischen Punkte in Bezug auf das «Ausspionieren der Kundenrechner» sind.

Aktivierung von Windows XP

Verschiedene Stellen behaupten, dass mit der Aktivierung von Windows XP über das Internet der Benutzer ausspioniert würde und dass zur Aktivierung persönliche Daten an Microsoft geliefert würden. Microsoft dagegen sagt, dass der Aktivierungsprozess absolut anonym ist und dass das Unternehmen im Rahmen des Aktivierungsprozesses keine Daten über den Benutzer sammle.

Prinzip der Windows-XP-Aktivierung

Für die Aktivierung von Microsoft Windows XP wird ein Freischalte-Code mit 50 Stellen per Telefon oder Internet

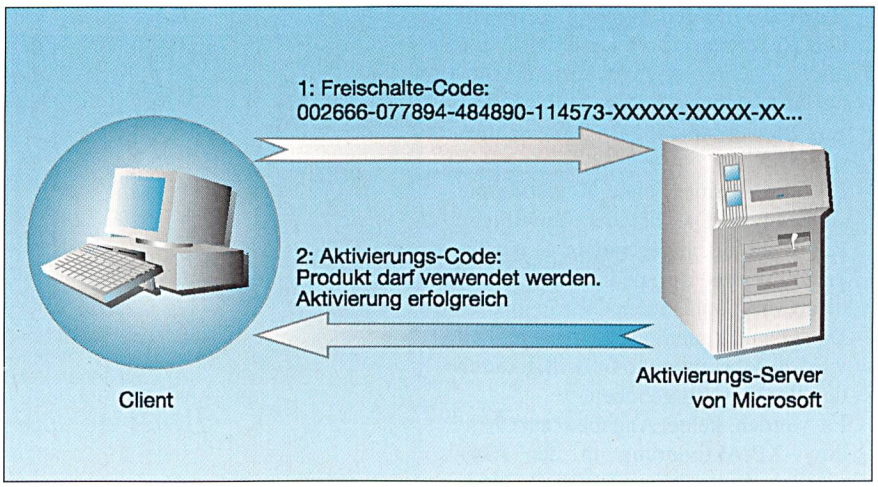


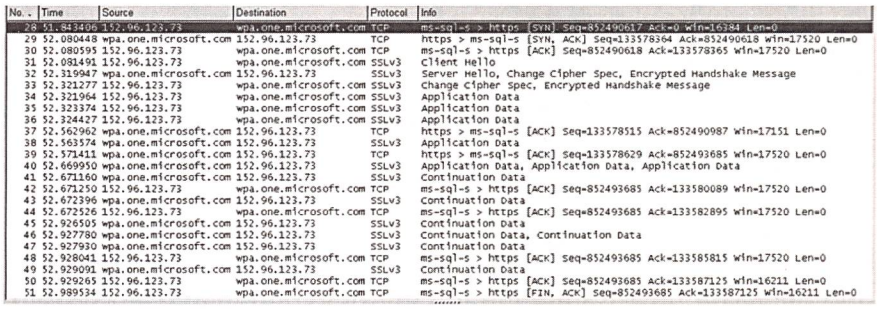
Bild 1 Prinzip des Aktivierungsprozesses von Microsoft

an Microsoft übermittelt, auf Grund dessen Microsoft entscheidet, ob das Produkt benutzt werden darf oder nicht (Bild 1). Falls es sich um ein rechtmässig erworbenes Produkt handelt, übermittelt Microsoft einen Aktivierungs-Code, nach dessen Eingabe die Software genutzt werden kann. Die Aktivierungs-Daten werden mittels http übermittelt und können somit problemlos die meisten Firewalls passieren.

Microsoft hat lange Zeit nicht genau bekannt gegeben, wie sich der Freischalte-Code zusammensetzt. Vor allem wurde nicht angegeben, welche Informationen über das PC-System im Freischalte-Code enthalten sind. Untersuchungen haben ergeben, dass der Freischalte-Code aus der Seriennummer der erworbenen Software und einem so genannten Hardware-Hash[1] besteht [1]. Die Seriennummer identifiziert die installierte Software eindeutig, nicht aber den Käufer: die Zuordnung zu Personen ist erst zusammen mit der Registrierung der Software möglich.

Gemäss Microsoft werden bei der XP-Aktivierung via Internet Datenmengen im Bereich von etwa 3 kB an Microsoft übertragen, was wesentlich mehr ist, als für die Übermittlung des 50-stelligen Freischalte-Codes nötig wäre [2]. Die offiziellen Angaben von Microsoft beschreiben aber, dass im Rahmen der Aktivierung auch gleich die freiwillige Registrierung vorgenommen werden kann und dass so die 3 kB zu Stande kommen. Microsoft erklärt die Aktivierung per Internet als unbedenklich und verweist auf eine Studie der TÜV Informationstechnik GmbH (TÜViT), welche die Produkte-Aktivierung betreffend Datenschutz überprüft hat [3]. Das Ergebnis dieser Studie sind folgende Aussagen (Zitate Microsoft [4]):

- Während der Aktivierung werden nur die Installations-ID (Produkt-ID und Hardware-ID) und, wenn eine freiwillige Registrierung gewählt wird, die im Assistenten angegebenen persönlichen Angaben an Microsoft übertragen. Die Übertragung findet verschlüsselt statt.
- Eine Aktivierung ohne Registrierung ist anonym. Die bei der freiwilligen Registrierung angegebenen Personaldaten werden mit den Aktivierungsdaten verknüpft in der Clearinghouse-Datenbank hinterlegt. In diesem Fall wird die Anonymität freiwillig durch den Benutzer aufgehoben.
- Es werden keine Angaben zur Windows-XP-Aktivierung in der Aktivierung von Office-XP/Visio-2002-Produkten verwendet und umgekehrt. Office-XP- und Visio-2002-Produkte verwenden die gleichen Hardware- und Benutzerangaben.
- Die Hardware-ID wird aus verschiedenen Hardware-spezifischen Angaben durch einen Hash-Algorithmus gebildet. Daher ist ein Rückschluss auf die Eigenschaften des Benutzer-PC (ausser des Vorhandenseins bestimmter Komponenten, wie z.B. Netzwerkadapter oder SCSI-Karte) seitens Microsoft nicht möglich. Andere Angaben, wie etwa der bei der Installation angegebene Benutzernamen oder andere Einträge der Registry, werden während Setup, Login und Aktivierung von den untersuchten Komponenten nicht an den Clearinghouse-Server übertragen.
- Eine Übertragung der Aktivierungs-/Registrierungsdaten findet erst nach einer expliziten Aufforderung durch den Benutzer statt («Weiter»-Knopf im Benutzeroptionen-Dialog). Aktivierungsangaben werden jedoch früher (teilweise während des Setups) verschlüsselt abgespeichert.
- Der Programmcode, der in der Aktivierung eine Rolle spielt (Bildung Hardware-ID, Übertragung der Daten an Clearinghouse, Assistent), wird in den Benutzer- und Clearinghouse-Clients als statischer Code in Executables oder DLL realisiert. Es gibt keine Codeteile, die über Internet heruntergeladen werden und dadurch unkontrollierte Änderungen beinhalten könnten.
- Auf Grund der eingesetzten Konfigurations-Kontrollmassnahmen sind bei Microsoft keine unbemerkten Änderungen am Quellcode oder den Endprodukten möglich.



No.	Time	Source	Destination	Protocol	Info
28	51.843406	152.96.123.73	wpa.one.microsoft.com	TCP	ms-sql-s > https [SYN] Seq=852490617 Ack=0 Win=16384 Len=0
29	52.080448	wpa.one.microsoft.com	152.96.123.73	TCP	https > ms-sql-s [SYN, ACK] Seq=133578364 Ack=852490618 Win=17520 Len=0
30	52.080595	152.96.123.73	wpa.one.microsoft.com	TCP	ms-sql-s > https [ACK] Seq=852490618 Ack=133578365 Win=17520 Len=0
31	52.081491	152.96.123.73	wpa.one.microsoft.com	SSLv3	Client Hello
32	52.319947	wpa.one.microsoft.com	152.96.123.73	SSLv3	Server Hello, Change Cipher Spec, Encrypted Handshake Message
33	52.321277	152.96.123.73	wpa.one.microsoft.com	SSLv3	Change Cipher Spec, Encrypted Handshake Message
34	52.321964	152.96.123.73	wpa.one.microsoft.com	SSLv3	Application Data
35	52.323374	152.96.123.73	wpa.one.microsoft.com	SSLv3	Application Data
36	52.324427	152.96.123.73	wpa.one.microsoft.com	SSLv3	Application Data
37	52.562962	wpa.one.microsoft.com	152.96.123.73	TCP	https > ms-sql-s [ACK] Seq=133578515 Ack=852490987 Win=17151 Len=0
38	52.563374	wpa.one.microsoft.com	152.96.123.73	SSLv3	Application Data
39	52.571411	wpa.one.microsoft.com	152.96.123.73	TCP	https > ms-sql-s [ACK] Seq=133578629 Ack=852493685 Win=17520 Len=0
40	52.669950	wpa.one.microsoft.com	152.96.123.73	SSLv3	Application Data, Application Data, Application Data
41	52.671160	wpa.one.microsoft.com	152.96.123.73	SSLv3	Continuation Data
42	52.671250	152.96.123.73	wpa.one.microsoft.com	TCP	ms-sql-s > https [ACK] Seq=852493685 Ack=133580089 Win=17520 Len=0
43	52.672396	wpa.one.microsoft.com	152.96.123.73	SSLv3	Continuation Data
44	52.672526	152.96.123.73	wpa.one.microsoft.com	TCP	ms-sql-s > https [ACK] Seq=852493685 Ack=133582895 Win=17520 Len=0
45	52.926505	wpa.one.microsoft.com	152.96.123.73	SSLv3	Continuation Data
46	52.927780	wpa.one.microsoft.com	152.96.123.73	SSLv3	Continuation Data, Continuation Data
47	52.927930	wpa.one.microsoft.com	152.96.123.73	SSLv3	Continuation Data
48	52.928041	152.96.123.73	wpa.one.microsoft.com	TCP	ms-sql-s > https [ACK] Seq=852493685 Ack=133585815 Win=17520 Len=0
49	52.929091	wpa.one.microsoft.com	152.96.123.73	SSLv3	Continuation Data
50	52.929265	152.96.123.73	wpa.one.microsoft.com	TCP	ms-sql-s > https [ACK] Seq=852493685 Ack=133587125 Win=16211 Len=0
51	52.989534	152.96.123.73	wpa.one.microsoft.com	TCP	ms-sql-s > https [FIN, ACK] Seq=852493685 Ack=133587125 Win=16211 Len=0

Bild 2 Aktivierung von Windows XP, verschlüsselt

Übertragene Informationen bei der Aktivierung von Windows XP

Bei den von der ITA-HSR durchgeführten Untersuchungen zur Windows-XP-Aktivierung wurde allerdings beobachtet, dass viel mehr als die von Microsoft angegebenen 3-kB-Daten abgeschickt werden. In der ersten Phase werden die erwarteten 3 kB an Microsoft gesendet. Danach wird die Verbindung zum Microsoft-Server[2] abgebaut. In einer zweiten Phase wird eine neue SSL-Verbindung[3] zum gleichen Server aufgebaut und es werden Daten im Umfang von rund 55 kB an Microsoft gesendet. Um welche Art Daten es sich dabei handelt, kann nicht gesagt werden, da sie wie erwähnt verschlüsselt übertragen werden und Microsoft nichts dazu bekannt gibt

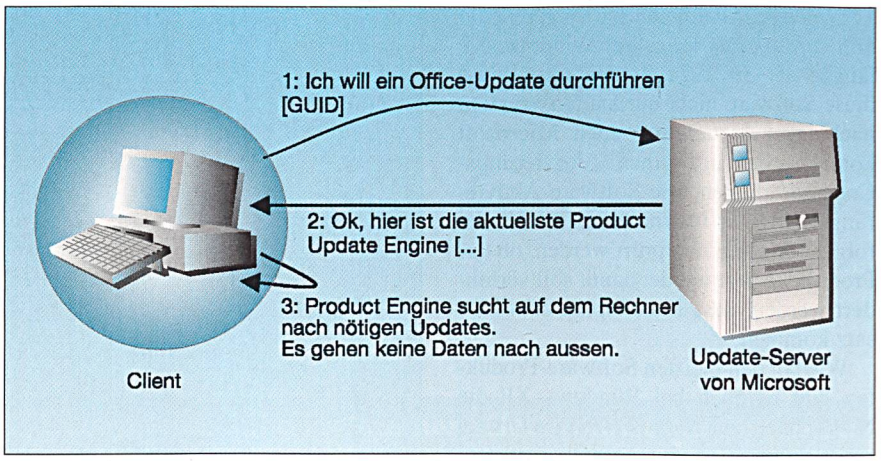


Bild 3 Ablauf internes Update

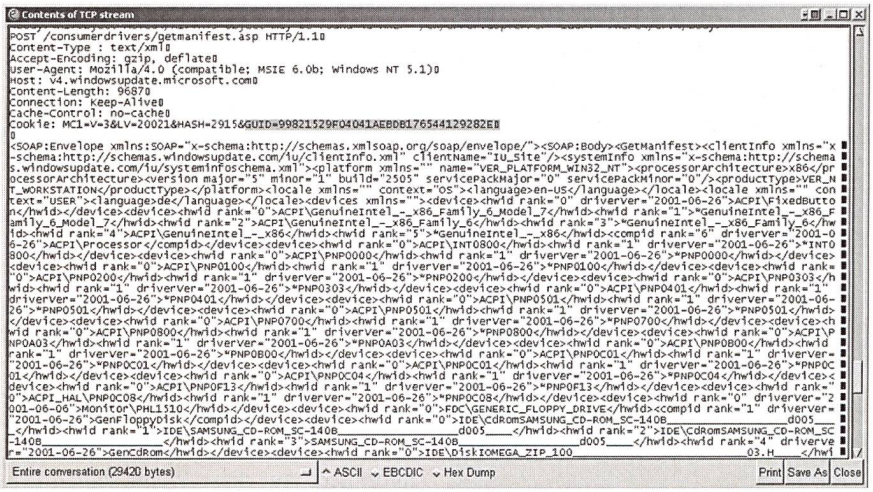


Bild 4 Auszug der Daten, die beim Update an Microsoft übermittelt werden

(Bild 2). Die TÜViT-Studie, von welcher nur ein Überblick öffentlich erhältlich ist, gibt auch keinen Hinweis auf den Inhalt dieser 55-kB-Daten.

Des Weiteren gibt es eine Analyse der Aussagekraft der TÜViT-Studie, welche zu einem ernüchternden Ergebnis kommt [5]. So wurden beispielsweise die verschlüsselt übermittelten Daten mit einem von Microsoft zur Verfügung gestellten Produkt analysiert, womit möglicherweise nur die offiziellen Registrierungs- und Aktivierungsdaten für TÜViT anzeigt und die anderen Informationen stillschweigend übersprungen werden konnten.

Weiter bemängelt die Analyse, dass die TÜViT-Prüfer die im Vergleich zu den angeblichen Nutzdaten «wesentlich grössere»[4] Datenmenge durchaus bemerkt hätten, ohne zu prüfen, ob dieses «wesentlich grösser» durch eine ineffiziente Protokollnutzung oder etwa durch «zusätzliche Nutzdaten» entstanden ist.

Nach den Untersuchungen des Aktivierungsprozesses bleibt daher ein «ungutes Gefühl» in Bezug auf die Aktivierung per Internet, weil unklar ist, welche Art Informationen zusätzlich zum 50-stelligen Freischalte-Code verschlüsselt an Microsoft verschickt werden. Wer also der Aktivierung über das Internet nicht traut, sollte die Aktivierung per Telefon vornehmen, wo nur der 50-stellige Freischalte-Code bekannt zu geben ist.

Übertragene Informationen bei der Aktivierung von Office XP

Mit dem Betriebssystem Windows XP wurde unter der Bezeichnung Office XP auch eine neue Version des Windows-Office-Pakets verfügbar. Office XP bringt gegenüber der Vorgängerversion Office 2000 Verbesserungen wie eine ergonomisch überarbeitete Benutzeroberfläche, höhere Betriebsstabilität, Smart Tags, Document Recovery sowie Send for Review.

Office XP arbeitet mit den gleichen Aktivierungs-Mechanismen wie für das Betriebssystem selbst. Es gibt einen 50-stelligen «Office-XP-Freischalte-Code», welcher per Internet oder Telefon an Microsoft übermittelt wird. Als Antwort erhält man den Aktivierungs-Code, falls Microsoft die entsprechende Software als «rechtmässige Installation» identifiziert hat.

Der Office-XP-Freischalte-Code setzt sich aus der Office-XP-Seriennummer und dem selben Hardware-Hash wie beim Windows-XP-Freischalte-Code zusammen.

Im Gegensatz zur Aktivierung von Windows XP wurden aber bei den vorliegenden Tests im Rahmen der Aktivierung von Office XP lediglich die von Microsoft angegebene Datenmenge von 3 kB und keine zusätzlichen Daten übermittelt.

Automatische Software-Aktualisierung

Oft entdecken Software-Firmen Fehler oder verbessern ihre bereits im Einsatz stehenden Produkte. Zur Korrektur von Fehlern bieten die Hersteller so genannte «Patches» (Flickwerk) an. Geht es um Erweiterungen oder Verbesserungen der Funktionalität, so spricht man eher von «Updates». Patches und Updates dienen damit der Verbesserung installierter Software-Produkte. Mit der generellen Vernetzung können Patches und Updates einfach via Internet bezogen werden.

Die meisten Anwender kümmern sich aber nicht um die Erneuerung ihrer Software. Aus diesem Grund haben viele Software-Hersteller automatische Update-Funktionen in ihre Programme eingebaut. Bei Microsoft-XP-Produkten untersucht eine so genannte «Product Update Engine» lokal, wie aktuell die installierten Produkte sind, indem sie die Kennung der aktuellen Installation mit der Kennung der neusten verfügbaren Installation vergleicht. Diese Product Update Engine wird von Microsoft geliefert, wenn sich jemand entscheidet, regelmässig solche Update-Checks durchzuführen (Bild 3).

Der Update-Server von Microsoft stellt auf Grund der Anfrage des Clients die benötigten Updates zur Verfügung. So hat der Client jeweils die aktuellste Update Engine lokal auf dem Rechner.

Falls die Product Update Engine feststellt, dass neuere Versionen der installierten Software verfügbar sind, meldet sie dies dem Benutzer und er kann selbst entscheiden, ob er den Aktualisierungsprozess starten will.

Übertragene Informationen bei der Aktualisierung von Windows XP

Windows XP unterstützt automatisches Update, d.h. bei ans Internet ange-

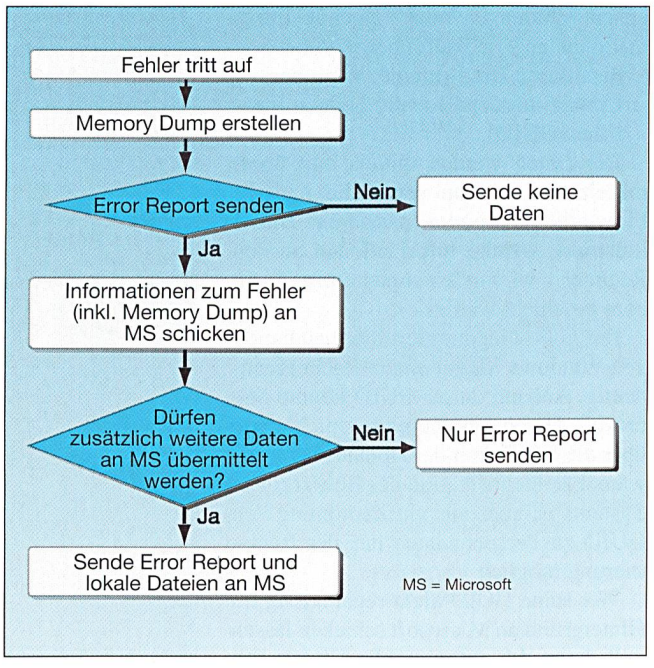


Bild 5 Ablauf des Error Reportings

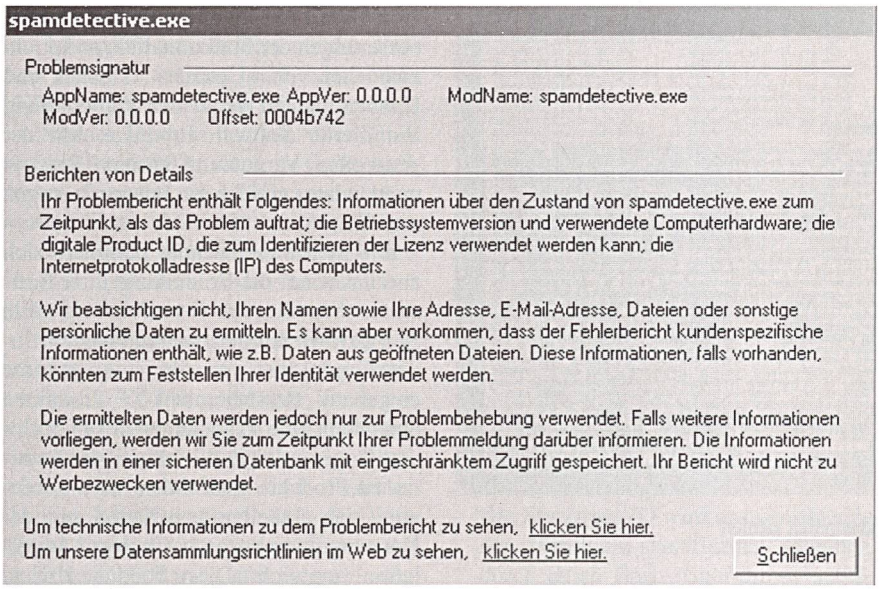


Bild 6 Error-Reporting-Richtlinien von Microsoft

schlossenen Rechnern sucht Windows XP periodisch nach neuen Versionen. Die Product Update Engine für das automatische Updating ist in der Windows-XP-Grundeinstellung bereits aktiviert, kann aber durch den Benutzer bewusst deaktiviert werden. Mit diesen Anfragen werden folgende Informationen mitgeschickt:

- GUID[5] des Produktes,
- ClassID der Update Engine (wird zur Versionsprüfung der Engine benötigt).

Sind Verbesserungen von Windows XP verfügbar, wird dies dem Benutzer mitgeteilt und er kann die Erneuerung mit wenigen Mausklicks veranlassen. Dazu werden zusätzlich von den vorangegangenen Meldungen noch folgende Informationen an Microsoft übermittelt:

- detaillierte Hardwareinformationen,
- Cookie mit der Globally Unique Identifier (GUID).

Die Daten werden mittels http übermittelt und können somit die meisten Firewalls problemlos passieren. Bild 4 illustriert, welche Informationen an den Rechner v4.windowsupdate.microsoft.com geschickt werden.

Die GUID identifiziert die Installation von Windows XP auf einem Rechner eindeutig. Anhand dieser GUID könnte Microsoft Daten sammeln, beispielsweise über die Häufigkeit der Updates der Software. Die Identifikation des Besitzers des Systems ist aber nur via Zuordnung von GUID zu Personendaten aus der Registrierung möglich.

Wer seine GUID nicht regelmässig im Hintergrund an Microsoft schicken lassen will, kann das automatische Update mit wenigen Mausklicks unterbinden. Er muss sich aber künftig selbst um die Aktualisierungen seiner Software kümmern, indem er regelmässig die entsprechenden Web-Seiten besucht und allenfalls Updates bezieht und installiert.

Übertragene Informationen bei der Aktualisierung von Office XP

Auch beim Update des Office-XP-Paketes wird die GUID an Microsoft übertragen. Dies erlaubt es Microsoft – auch bezüglich Office XP – Buch darüber zu führen, welcher Rechner welche Version installiert hat und wie oft Office-XP-Updates durchgeführt werden.

Bei den Untersuchungen dieses Office-XP-Update-Prozesses wurden aber ausser der GUID keine Übermittlungen weiterer Daten an Microsoft beobachtet.

Error Reporting

Error-Reporting-Ablauf

Mit Error Reporting verfügt Windows XP über einen neuen Mechanismus, der beim Auftreten eines Fehlers beim Betriebssystem oder bei irgendeinem Anwenderprogramm in Aktion tritt und Microsoft über allfällige Softwareprobleme informiert. Auf diese Weise sollten Programmfehler entdeckt und schnell behoben werden können. Der Ablauf des Error Reporting ist in Bild 5 dargestellt.

Das Betriebssystem detektiert Fehlfunktionen und erstellt automatisch einen Memory Dump, sobald ein Fehler aufgetreten ist. Anschliessend wird der Benutzer gefragt, ob er einen Error Report an Microsoft senden möchte. Entscheidet sich der Benutzer, keine Daten zu senden, so wird der Vorgang an dieser Stelle abgebrochen und der Memory Dump gelöscht. Andernfalls sendet das Error Reporting Tool den Memory Dump sowie zusätzliche Informationen über den Fehler an Microsoft. Falls Microsoft für die Bearbeitung des Error Reports noch weitere Informationen benötigt, so wird angefragt, ob noch zusätzliche lokale Dateien heruntergeladen werden dürfen.

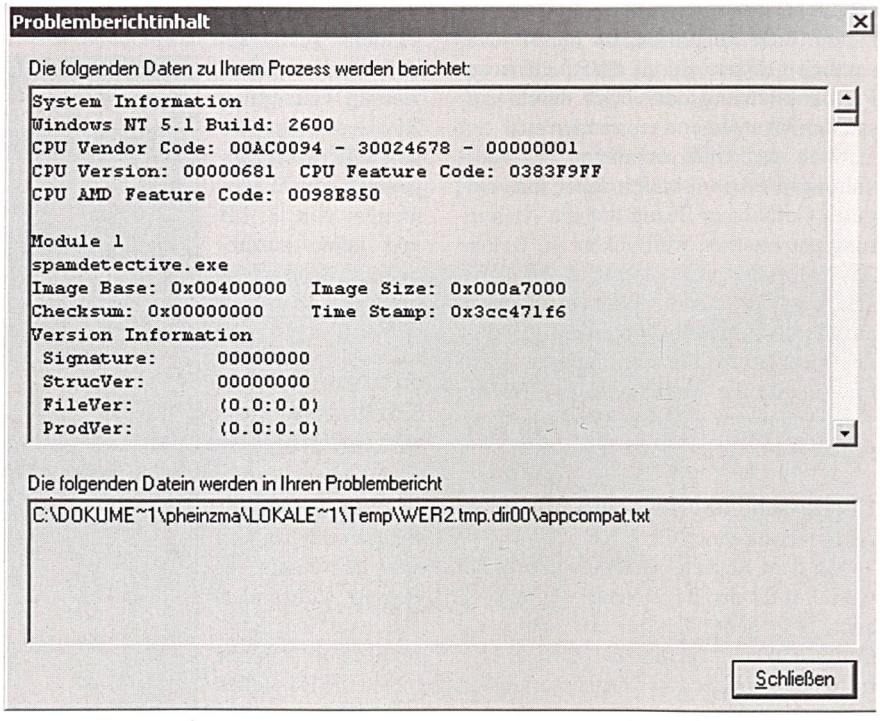


Bild 7 Error-Report-Begleitinformationen von Microsoft

Dafür zeigt eine Dialogbox die Namen aller noch benötigten Dateien an, so dass der Benutzer entscheiden kann, ob diese Dateien an Microsoft gesendet werden dürfen oder nicht.

Microsoft gibt an, dass sich im Memory Dump vertrauliche Daten befinden könnten, weist aber darauf hin, dass diese Daten nicht weiter verwendet werden [6]. Ausserdem erteilt Microsoft nach eigenen Aussagen nur wenigen Mitarbeitern Zugriff auf die Error Reports [7].

Bei den zusätzlichen Daten, die mit dem Memory Dump mitgeschickt werden, handelt es sich laut Microsoft [6] um:

- Informationen über den Fehler (Instruktion, die den Fehler verursacht hat),
- Version des Betriebssystems,
- Prozessor-Typ,
- Liste aller laufenden Module (DLL),
- Liste aller Threads (Context + Stack),
- globale Daten.

Was unter den «globalen» Daten zu verstehen ist, gibt Microsoft nicht genauer bekannt. Wie bereits erwähnt, kann Microsoft bei einem schweren Fehler den Benutzer anfragen, ob noch weitere Daten vom Rechner an Microsoft übertragen werden dürfen. Dabei handelt es sich um Informationen wie:

- das beim Auftreten des Fehlers bearbeitete Dokument,
- verschiedene Registry-Einträge,
- Systemdateien (wie beispielsweise die geladene DLL).

Dabei ist zu beachten, dass sich im aktuellen Dokument eventuell Firmengeheimnisse oder geheime Passwörter befinden und dass mit Hilfe der Registry-Einträge diese Daten sehr einfach einer Person zugeordnet werden können, da diese Einträge den Namen des Benutzers enthalten können.

Als Gegenleistung für das Senden von Error Reports an Microsoft erhält der Benutzer in einem ersten Schritt einen Link, unter welchem die Lösung zu seinem Problem beschrieben ist. Dies ist natürlich nur möglich, wenn es ein bekanntes Problem ist und Microsoft eine Lösung dafür bereitstellt. Später wird der Benutzer gegebenenfalls von einem Patch oder einer neuen Version seines Programms profitieren können.

Bei allen Error Reports hat der Benutzer jedoch die Möglichkeit, das Senden an Microsoft zu verbieten, indem er die entsprechenden Fragen jeweils verneint. Erlaubt der Benutzer dem Betriebssystem das Senden der Daten nicht, werden tatsächlich auch keine Informationen an Microsoft übertragen.

Wie weiter unten noch gezeigt wird, kann das Betriebssystem so eingestellt werden, dass keine Error Reports erstellt werden [8].

Error-Reporting-Beispiel

Im folgenden Beispiel wurde ein Error-Report für die Anwendung «spam detective.exe» provoziert (Bild 6). Nach Auftritt des Fehlers kann der Benutzer entscheiden, ob er einen Error Report senden will oder nicht. Als Information von Microsoft über die zu sendenden Daten lassen sich folgende Zusatzinformationen darstellen. Dabei wird klar beschrieben, dass keine persönlichen Daten ermittelt werden.

In den technischen Informationen wird ferner im Problembericht (Bild 7) offen gelegt, welche Daten mit dem Memory Dump an Microsoft geschickt werden.

Da die Error-Reporting-Daten verschlüsselt übertragen werden und Microsoft keine Angaben über die Datenmenge macht, kann weder über den Inhalt noch über die Menge der übermittelten Daten eine Aussage gemacht werden.

Verwendung von Cookies

Cookies sind Datensätze, welche ein Web-Server beschreiben und im Browser des Kundenrechners abspeichern kann.

Beschreibung des Dienstes	Welche Daten werden übermittelt?	Defaulteinstellung (Veränderungsmöglichkeit)	Einsatz von Cookies	Kommentar
Windows-XP-Aktivierung Die Aktivierung muss durchgeführt werden, damit das Betriebssystem länger als 30 Tage eingesetzt werden kann.	Bei Aktivierung via Internet: Freischalte-Code (Serienummer und Hardware-Hash), Zertifikate und zusätzlich Daten in verschlüsselter Form im Umfang von 50 kB. Bei telefonischer Aktivierung: nur Freischalte-Code (Seriennummer und Hardware-Hash).	Eingeschaltet bei Aktivierung über Internet (lässt sich deaktivieren).	Nein	Telefonische Aktivierung ist unproblematisch. Bei der Aktivierung via Internet muss man Microsoft glauben, dass wirklich keine sensitiven Daten vom Rechner zu Microsoft übertragen werden.
Office-XP-Aktivierung Die Aktivierung muss durchgeführt werden, damit die Software überhaupt bzw. länger als 30 Tage eingesetzt werden kann.	Daten im Umfang von rund 3 kB (Inhalt kann nicht bestimmt werden, da verschlüsselt).	Aktivierung über Internet (lässt sich deaktivieren, auch wenn Rechner am Internet angeschlossen ist).	Nein	
Windows XP Update XP sucht nach Updates und installiert diese.	Hardware-Informationen, GUID und Versionsnummer.	Eingeschaltet (lässt sich deaktivieren).	Ja (Global Cookie)	Ausser der GUID werden keine sensitiven Daten übertragen.
Office XP Update	Nur die GUID (es werden lediglich Product-Update-Dateien empfangen und automatisch installiert).	Ausgeschaltet (lässt sich nicht automatisieren).	Ja (Global Cookie)	
Error Reporting	Systeminformationen und Memory Dump (kann eventuell aktuell bearbeitete Dokumente enthalten).	Eingeschaltet (lässt sich mit speziellem Tool bzw. Registry-Eintrag-Änderung deaktivieren).	Nein	Kritisch, da im an Microsoft geschickten Memory Dump Informationen aus aktuellen Dokumenten enthalten sein könnten.

Tabelle Zusammengefasste Ergebnisse der Untersuchung

Beim nächsten Zugriff auf den Server schickt der Browser den Datensatz zum Server, so dass dieser die beim letzten Besuch des Kunden abgespeicherten Informationen wieder abrufen kann. Auf diese Weise bringen Cookies Gedächtnis ins Web.

Windows XP arbeitet für die Aktualisierung mit so genannten «Global Cookies», in welchen die Windows-XP-Produkt-ID des Kundenrechners abgespeichert wird. So lässt es sich einfach feststellen, zu welcher Windows-XP-Installation eine Aktualisierung gemacht wurde, welche Version aktuell auf dem Rechner installiert ist und wie häufig Anfragen nach Aktualisierungen gemacht werden.

Die Windows-XP-Cookies haben bis zu mehreren Monaten Gültigkeit. Falls ein Kundenrechner keine Cookies akzeptiert, dauert der Aktualisierungsvorgang eventuell ein wenig länger, da Microsoft nicht sofort sagen kann, ob die neuesten Softwareversionen auf dem Rechner installiert sind. Es müssen dann mehrere Informationen an Microsoft übertragen werden, was ein wenig Zeitverlust bedeuten kann. Dafür kann das Verhalten des Benutzers nicht ganz so einfach protokolliert werden.

Gegenmassnahmen

In der Tabelle sind die Ergebnisse der Untersuchung zusammengefasst.

Grundsätzlich hat sich zwar gezeigt, dass Microsoft recht transparent über ihre Kommunikationsarten mit den Kundenrechnern informiert und mittlerweile in Bezug auf Datenschutzfragen recht sauber arbeitet, doch lässt sich daraus keineswegs schliessen, dass dies alle Software-Hersteller tun. In [9] wurden einige häufig verwendete Tools genauer unter die Lupe genommen, und es hat sich gezeigt, dass manche Hersteller mehr über den Benutzer in Erfahrung bringen wollen, als diesem bewusst sein dürfte.

Wer sich durch die Kommunikationsprozesse mit den Software-Herstellern «ausspioniert» fühlt, hat verschiedene Möglichkeiten, sich dagegen zu schützen.

Auch mit Hilfe einer Personal Firewall liessen sich unerwünschte Anfragen blockieren. Die optimale Konfiguration der Personal Firewall überfordert aber viele Normalanwender, weshalb diese Massnahme nicht für alle geeignet ist.

Software-Aktivierung und -Registrierung

Die Aktivierung von Software kann nicht ausgeschaltet werden. Der Benutzer kann aber entscheiden, ob die Software über das Internet oder telefonisch aktiviert werden soll. Um sicher zu gehen, dass nur die minimal benötigten Informationen an Microsoft gelangen, empfiehlt es sich, die Aktivierung per Telefon zu vollziehen.

Wer seine Software nicht registrieren lassen will, kann dies durch Drücken des «Abbrechen»-Knopfes bei der entsprechenden Aufforderung erreichen.

Software-Aktualisierung

Um das regelmässige Anfragen bezüglich allfälliger Updates des Betriebssystems auszuschalten, müssen Anpassungen in der Registry vorgenommen werden. Das Freeware Tool XP-AntiSpy [8] besorgt die entsprechenden Registry-Änderungen für den Benutzer (Bild 8).

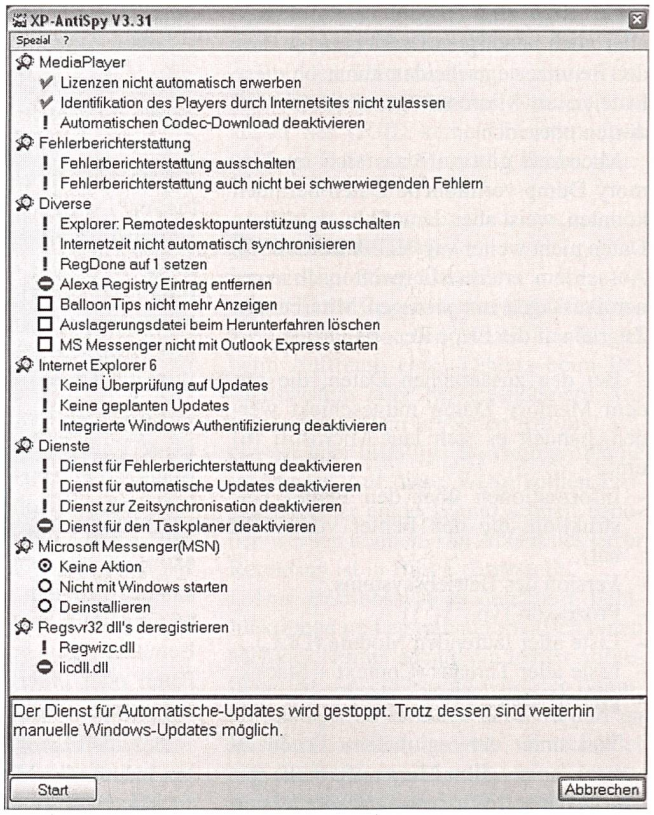


Bild 8 Beispiel XP-AntiSpy, www.xpantispy. de

Error Reporting

Das bei Fehlfunktionen von Betriebssystem oder Applikationen automatisch ausgelöste Error Reporting kann der Benutzer durch Drücken des «Don't Send»-Knopfs unterbinden. Auch hier reduziert das Tool XP AntiSpy das Mitteilungsbedürfnis von Windows XP, indem es das Error Reporting dauerhaft ausschaltet.

Referenzen

[1] Fully Licensed GmbH: Untersuchung des Freigabecodes. www.licenturion.com/xp/wpa-ger.txt

[2] Microsoft: Microsoft Windows Product Activation. Technisch, www.microsoft.com/germany/themen/piraterie/produktaktivierung/WPA_technisch.doc

[3] TÜViT: Studie zur Microsoft-Produktaktivierung. www.tuvit.de/XS/ASP/content.000203/sprache.DE/SX/

[4] Ergebnis Technische Studie auf der Microsoft-Seite, www.microsoft.com/germany/themen/piraterie/produktaktivierung/tuev/techerg.htm

[5] Analyse des TÜViT-Berichts, www.redtenbacher.de/security/wpa.htm#schwachstellen

Windows XP – un espion?

Transmission de données lors de l'activation et de la mise à niveau du logiciel

Les logiciels modernes sont distribués, activés, renouvelés et entretenus par voie électronique. Dans le cadre du nouveau système d'exploitation Windows XP, on reproche souvent à Microsoft d'utiliser les liaisons Internet non seulement pour l'activation, le renouvellement et l'amélioration du logiciel installé mais également pour recueillir des informations concernant l'utilisateur et la configuration de son système. Afin de placer ces critiques dans l'optique adéquate, l'Institut de technologies et d'applications Internet de la haute école de Rapperswil (ITA-HSR) a examiné les données réellement envoyées par Windows XP à Microsoft sur Internet lors de l'activation et de la mise à niveau.

[6] Microsoft: Microsoft Error Reporting Data Collection Policy. http://watson.microsoft.com/dw/1033/dcp.asp
[7] Microsoft: End User Privacy Policy in Application Error Reporting. http://support.microsoft.com/default.aspx?scid=kb;EN-US;q283768
[8] XP-AntiSpy Tool, www.xpantispy.de
[9] ITA-HSR: Untersuchung von häufig eingesetzten Tools im Bezug auf Spionage von Benutzerdaten. www.ita.hsr.ch

Links

IT News: Aktivierungsinformationen von Microsoft. http://cad-school.ch/News/Software/Microsoft/XP-Aktivierung/aktivierungsinfos.html
ZDNet-Artikel über Error Reporting, www.zdnet.com/zdnn/stories/news/0,4586,5098483,00.html
Computer Incident Advisory Capability Information Bulletin about Office XP Error Reporting, http://ciac.org/ciac/bulletin/m-005.shtml
Heise.de: Windows nährt Schnüffelvorwürfe. http://heise.de/ct/02/02/048
Vorn Forum: Office XP Registrierung – Welche Angaben speichert Microsoft. http://vorn.de/php/content/showthread.php?threadid=128

Angaben zu den Autoren

Prof. Dr. ***Peter Heinzmann*** ist seit 1991 Professor an der Hochschule Rapperswil (HSR), wo er auch das Institut für Internet-Technologien und -Anwendungen (ITA-HSR) aufgebaut hat. 1995 gründete er die auf Internet-Sicherheit spezialisierte Firma cnlab AG, ebenfalls mit Sitz in Rapperswil. *Kontakt: Institut für Internet-Technologien und -Anwendungen, Hochschule Rapperswil (ITA-HSR), peter.heinzmann@cnlab.ch*

Marcel Liebi, Informatik-Ing. FH, hat im Januar 2002 an der Hochschule Rapperswil seinen Abschluss gemacht. Er ist seither am Institut für Internettechnologien und -Anwendungen der Hochschule Rapperswil tätig und beschäftigt sich dort vorwiegend mit Internet-Sicherheit. *Kontakt: Institut für Internet-Technologien und -Anwendungen, Hochschule Rapperswil (ITA-HSR), mliebi@hsr.ch*

[1] Der Hardware-Hash wird über eine so genannte Einweg-Funktion (MD5) aus zehn verschiedenen Hardwaremerkmalen des Rechners bestimmt, auf dem das Betriebssystem installiert wurde – wozu auch Parameter der Graphikkarte und des IDE-Adapters[6] gehören. Er hängt zudem von der MAC-Adresse[7] des Netzwerkadapters und der Seriennummer des Prozessors ab. Aus dem Hardware-Hash lassen sich diese Merkmale jedoch nicht ableiten. Hardware-Hash und Freischalte-Code erlauben daher keine Rückschlüsse auf die eingesetzte Hardware.

[2] wpa.one.microsoft.com

[3] SSL: Secure Sockets Layer, www.openssl.com

[4] Gemäss dem ZDF-Magazin WISO immerhin die zwanzigfache Datenmenge an Protokolldaten gegenüber den offiziellen Nutzdaten.

[5] GUID: Globally Unique Identifier. Im Active Directory werden diese für die einzelnen Objekte benötigt. Auch bei der Installation von Produkten werden solche GUID verwendet, um die Programme eindeutig identifizieren zu können. Dabei handelt es sich um eine 128-Bit-Zahl, die aus verschiedenen Informationen gebildet wird. So wird unter anderem die MAC-Adresse[7] der Netzwerkkarte bei der Erstellung einer GUID verwendet, um sicherzustellen, dass die GUID weltweit eindeutig ist. Bei der Installation eines Betriebssystems wird auch eine GUID erstellt, die dann eine bestimmte Maschine identifiziert.

[6] IDE: Integrated Device Equipment. Schnittstellen-Standard für AT-Bus-Festplatten.

[7] MAC-Adresse: Angaben zu Hersteller und Typ der Netzwerkkarte. Sie identifiziert eine Netzwerkkarte weltweit eindeutig.