Warum ich XP-Antispy nicht mag
Eine Auseinandersetzung mit einem sehr populären Programm

Immer wieder liest man in so genannten „Fachzeitschriften“, Internetforen, auf „Tipps- und-Tweaks“ Seiten oder im Usenet Aussagen wie „XP-Antispy ist das Erste, was nach der Installation von XP draufkommt“, „Ohne XP-Antispy spioniert dich Windows gnadenlos aus“ oder auch „XP-Antispy macht Windows sicherer“.

Das klingt, zumal es so oft zu lesen ist, schon sehr beeindruckend und scheint zu bestätigen, dass XP-Antispy tatsächlich ein unverzichtbares Werkzeug für jeden Benutzer von Windows XP ist. Leider ist das aber absoluter Unfug, geboren aus Verunsicherung, Desinformation und schlichter Panikmache.

Historisches

XP kam im Oktober 2001 auf den Markt und war das erste Betriebsystem von MS, welches einen rudimentären Kopierschutz in Form der sagenumwobenen Produktaktivierung aufwies. Nachdem sich MS zu den technischen Details Aktivierung und zu den übertragenen Daten weitgehend ausschwieg, kamen schnell Gerüchte auf, dass weitaus mehr Daten als unbedingt notwendig bei der Onlineaktivierung zu MS gesendet werden würden. Dabei vermutete man auch, dass persönliche Daten ausspioniert werden würden. Welche persönlichen Daten ein frisch installiertes XP allerdings senden sollte, ist bis heute eine Frage, die von den Verfechtern dieser Theorie nicht beantwortet werden kann. Infolge dieser Unsicherheit wurden allerdings auch viele der sinnvollen Features von XP, die eine Online-Verbindung verwenden, pauschal verteufelt.

Natürlich soll nicht verschwiegen werden, dass Microsoft einige Fehler gemacht hat, die massiv zum schlechten Image und zur Verunsicherung in Bezug auf die Zwangsaktivierung beitrugen. Beispiele dafür sind die GUID in Office Dokumenten , über die der Autor dank der eingebetteten MAC Adresse weltweit hätte identifiziert werden können oder auch die absolut überzogenen Formulierungen in den Lizenzbedingungen des Media Players 7.1. Trotzdem sollte man sich die Funktionen, deren Deaktivierung XP-Antispy anbietet, einmal unvoreingenommen ansehen, bevor man sich durch den unbedachten Einsatz dieses Tools sein XP unbrauchbar macht.

Gehen wir also mal durch, was da alles zur Deaktivierung angeboten wird:

Der Mediaplayer.

Alle Einstellungen, die diesbezüglich in XPAntispy zu finden sind, lassen sich genau so gut in den Registern, die sich unter "Extras-->Optionen" direkt im Mediaplayer finden, tätigen.

Was im Einzelnen am automatischen Download von fehlenden Codecs oder am Abruf von Metadaten verwerflich ist, erschließt sich mir nicht wirklich, denn auch Player wie Winamp oder Ripper wie CDEx rufen Mediendaten von Datenbanken wie CDDB oder FreeDB ab. Ist dieses Verhalten dort jemals kritisiert worden? Auch Winamp will per Default Informationen über das Nutzerverhalten an Nullsoft schicken und dies lässt sich dort genau so einfach deaktivieren wie im Media Player. Trotzdem stand und steht Winamp weitaus weniger in der Kritik als der MediaPlayer.

Interessant ist, wie bei XP-Antispy manche Einstellung begründet wird. Der Grund dafür, dass Mediadaten nicht zur Mediadatenbank hinzugefügt werden sollten, soll sein, dass diese vermutlich über das Internet ausgelesen werden könnten. Wie das allerdings möglich sein soll oder welche Anhaltspunkte dafür existieren, steht nicht dabei.

Fehlerberichte

Keine Frage, hier besteht in seltenen Fällen ein Risiko, denn prinzipbedingt finden sich in einem Dump des Hauptspeichers unter ungünstigen Umständen auch Teile von aktuell bearbeitetet Dokumenten. Inwieweit diese verwertbar sind, sei mal dahingestellt, in einer vernetzten Umgebung will man aber mit Sicherheit nicht, dass solche Berichte das eigenen Netzwerk verlassen. Von daher deaktiviert man das einfach per Rechtsklick auf Arbeitsplatz -->Eigenschaften-->Erweitert-->Fehlerberichterstattung. Oder per Gruppenrichtlinie im Netzwerk.

Diverse Einstellungen

Der Autor von Antispy hat diese Sektion inzwischen mit dem Hinweis versehen, dass hier nicht alle Einstellungen sicherheitsrelevant sind. Welche er aber im Einzelnen nicht dieser Kategorie zuordnet, schreibt er leider nicht. Davon abgesehen ist die Sinnhaftigkeit der meisten Einstellungen durchaus zweifelhaft.

- "Remote Desktop Unterstützung ausschalten“ schaltet eben nicht den Remote Desktop ab, sondern verhindert nur das Senden von Remoteunterstützungsanfragen.

- "Zeit nicht automatisch über das Internet synchronisieren": Unixoide Systeme synchronisieren schon seit Jahrzehnten ihre Zeit per NTP. Wenn Windows das allerdings anbietet, muss es deaktiviert werden? Was NTP ist, wie es funktioniert und was dabei für Daten übertragen werden, findet sich übrigens in RFC958 (http://rfc.net/rfc958.html)

- "RegDone auf 1" setzen hat genau welchen Sinn? Dass man nicht mehr an die fällige Aktivierung erinnert wird?

- "Balloon-Tips nicht mehr anzeigen": Kann man machen. Mag für den ein oder anderen sinnvoll sein. Ist ja auch nur ein Schlüssel in der Registry
http://support.microsoft.com/?kbid=307729

- "Auslagerungsdatei beim Herunterfahren löschen": Eine sehr "*beliebte*" Einstellung, denn es kommen danach regelmäßig die Fragen, warum das Herunterfahren des Rechners auf einmal so lange dauert… Hintergrund der Einstellung ist wohl, dass ein anderer lokaler Benutzer unter bestimmten Umständen Datenfragmente aus der Auslagerungsdatei auslesen könnte. Die Wahrscheinlichkeit allerdings, an interessante Daten zu kommen, ist in den allermeisten Fällen durchaus als sehr gering einzustufen.

- "Messenger nicht mit Outlook starten" lässt sich bequem in Outlook festlegen, wenn man den Messenger nicht sowieso gleich deinstalliert, wie es seit SP 1 bequem möglich ist.

- "Bandbreitenbeschränkung aufheben": Ist glatter Blödsinn. Zitat aus http://support.microsoft.com/?kbid=316666 : "**Richtigstellung einiger falscher Behauptungen zur QoS-Unterstützung unter Windows XP**

In diversen Veröffentlichungen in Fachzeitschriften und Newsgroups wurde die Behauptung aufgestellt, dass Windows XP immer 20 Prozent der verfügbaren Bandbreite für QoS reserviert. Dies ist nicht der Fall.“

- "Schnelles Herunterfahren aktivieren": Ist eine der Quellen für z.B. „Beim Booten erhalte ich die Meldung, dass die Datei "c:\windows\system32 \config\system" beschädigt sei oder fehle“. Es wird ein Registry Key gesetzt, dafür sorgt, dass scheinbar nicht mehr reagierende Tasks rigoros beendet werden. Wird der Task, der für das Sichern der Registry auf die Platte zuständig ist, so beendet, zerlegt man sich ebenjene und darf sich auf eine Neuinstallation einrichten. Natürlich gibt es für das Problem auch noch andere Ursachen wie Hardwareprobleme und es tritt auch nicht auf allen Systemen auf, aber man sollte es auch nicht unnötig herausfordern, denn auf normal funktionierenden Systemen hat man keine positiven Effekte durch das Setzen dieses Keys.

- "Computer im Netzwerk nicht anzeigen" macht wann Sinn? Im Firmennetzwerk erledigt das der Admin, wenn es gewünscht ist, im Heimnetzwerk verzweifeln die Anwender, wenn sie die anderen Rechner nicht in der Netzwerkumgebung sehen. Die Erläuterung in Antispy ist durchaus witzig, denn der Computername ist für einen Angreifer wohl das letzte, wonach er sucht. Portscanner kümmern sich nicht um Computernamen, die sowieso nicht über das Internet sichtbar sind. Auf einer LAN-Party mag das anders sein, allerdings geht auch dort vom Computernamen wohl die geringste Gefahr aus. Wer nicht will, dass sein Rechner in so einem Netzwerk sichtbar ist, sollte besser nicht dahingehen. Schließlich ist der Rechner ja immer über seine IP Adresse erreichbar. IMHO wird mit dieser Einstellung eine Scheinsicherheit vorgegaukelt.

- "Aufruf von Regedit nicht zulassen": Auch hier ist der Sinn wohl eher fraglich. Im Netzwerk macht das der Admin per GPO, im Heimnetzwerk sperrt sich der Anwender nur von diesem Werkzeug aus. Viren und Würmer kümmern sich sowieso nicht darum, sondern setzen im Gegenteil selber diesen Schlüssel, um ihre Entfernung zu erschweren. Wer nicht will, dass "Unbefugte" Regedit benutzen, gibt ihnen keine Adminrechte an seinem PC.

- "Scripting Host deaktivieren" Muss jeder für sich selber entscheiden. Sicherheitstechnisch sinnvoller ist es, den Scripting Host aktiviert zu lassen und stattdessen nicht mehr als Admin zu arbeiten.

- "Beim Anmelden zuletzt eingeloggten User nicht anzeigen": Im Firmennetzwerk erledigt das der Admin per Gruppenrichtlinie, im Heimnetzwerk muss das natürlich jeder für sich wissen.

- "*.lnk, *.pif, *.scf und *.url Dateiendung anzeigen": Macht bei den drei letzteren durchaus Sinn, bei .lnk werden alle Links zu Programmen/Dateien z.B. auf dem Desktop als Tralalla.lnk angezeigt, was durchaus störend sein kann. Muss aber auch wieder jeder selber wissen. Sicherer wäre es jedenfalls, nicht einfach blind alle Dateien, die einem per Mail so zugeschickt werden, auszuführen…

- "Kein Autostart für CDs": Geschmacksache. Auf jeden Fall verursacht das keine Probleme, kann man also bedenkenlos machen.

- "Verlauf der zuletzt geöffeneten Dokumente löschen": Ebenfalls Geschmacksache und problemlos.

- "Bekannte Dateiendungen ebenfalls anzeigen": Sehr sinnvolle Einstellung. Mache ich standardmäßig auf jedem Rechner.

Zusammenfassend muss ich leider sagen, dass sich in dieser Kategorie überwiegend sinnlose oder falsche Einstellungen finden. Die wenigen, die tatsächlich Sinn machen, gehen darin fast unter..

Internet Explorer

Ich selber empfehle ja immer wieder, den IE nur für Aufgaben wie z.B. WindowsUpdate oder die Verwaltung des SUS zu verwenden, die mit anderen Browsern mangels ActiveX Unterstützung einfach nicht darstellbar sind. Das gilt auch für den IE nach XP SP2, obwohl Microsoft damit tatsächlich sehr weitgehende Verbesserungen in Sicherheitsbereich vorgenommen hat. Zumindest sind wohl alle bislang bekannten Sicherheitslücken gestopft worden; ob jedoch die zugrunde liegenden Probleme tatsächlich vollständig ausgeräumt wurden, darf bezweifelt werden.

Davon abgesehen, lassen sich alle von XP-Antispy vorgeschlagenen Einstellungen bequem im IE unter Extras-->Internetoptionen-->Erweitert tätigen. Ausgenommen die Erhöhung der maximal möglichen Connections. Hier hält sich der IE übrigens genau an die Vorgaben von RFC2616 und RFC1945. Wer das trotzdem ändern will und eventuelle Probleme auf Serverseite in Kauf nimmt: http://www.faqweb.de/tip0485.htm

BTW: Wer alle von XP-Antispy angebotenen Optionen in diesem Bereich aktiviert, wird den IE so oder so nicht mehr verwenden wollen/können. Ohne ActiveX und Javascript lassen sich inzwischen kaum noch Seiten mit dem IE vernünftig darstellen.

Dienste

Am einfachsten lässt sich alles, was XP-Antispy hier vorschlägt, per Rechtsklick auf Arbeitsplatz-->verwalten-->Dienste und Anwendungen-->Dienste erledigen. Aber warum überhaupt? Gehen wir die Dienste mal durch:

- "Dienst für Fehlerberichterstattung": Kann man machen, wenn man lieber ohne jede Meldung über abstürzenden Anwendungen bleiben will und mit der dadurch komplizierteren Fehlersuche leben kann. Deaktiviert hat man das Senden der Fehlerberichte ja bereits unter Punkt 2.

- "Dienst für automatische Updates deaktivieren": Damit sperrt man sich effektiv von Windows Update aus. Die aktuelle Version (v5) setzt einen laufenden Windows Update Dienst voraus. Siehe
http://v5.windowsupdate.microsoft.com/v5consumer/showarticle.aspx?articleid=8&ln=de

Früher konnte man, wenn man regelmäßig mindestens alle 2 Wochen Windows Update besuchte und sich die wichtigen Patches installierte, diesen Dienst deaktivieren. Heute sollte man ihn so konfigurieren, dass man automatisch über verfügbare Updates informiert wird.

MS reagiert hier auf die Erfahrungen der Vergangenheit, die zeigten, dass sehr viele Anwender nicht in der Lage oder Willens waren, Windows Update regelmäßig mindestens einmal im Monat zu besuchen.

Wie ich zu der Aussage komme? Am 11. August 2003 wurde das Internet von einer Welle ohnegleichen in Form des MSBlaster/Lovesan Wurmes überschwemmt. Der Patch, der die Sicherheitslücke stopfte, die von diesem Wurm ausgenutzt wurde, war seit 16 Juli 2003, also knapp 4 Wochen vorher per Windows Update verfügbar. Hätten alle diese Anwender den Dienst aktiviert gehabt, wäre Lovesan nicht einmal eine Randnotiz wert gewesen.

Man sollte denken, dass die Anwender daraus gelernt haben. Das wäre allerdings ein Irrtum, denn im Jahr 2004 wiederholte sich dieses Spiel mit einem neuen Wurm namens Sasser.

Dieser Dienst wählt sich auch nicht von alleine bei MS ein, sondern nutzt eine bestehende Onlineverbindung, um darüber mit niedriger Priorität und Bandbreite die zur Verfügung stehende Updates herunterzuladen. Dabei werden keine anderen Daten als beim Besuch von Windows Update übertragen. Nach erfolgreichem Abschluss werden diese nicht automatisch installiert, sondern der Anwender wird explizit gefragt. Wo ist also das Problem? Doch wohl schlimmstenfalls darin, dass man Windows Update scheinbar grundsätzlich nicht vertraut. Wer sich wirklich in Ruhe damit auseinandersetzten will, findet hier ausreichend Information:

http://v5.windowsupdate.microsoft.com/v5consumer/privacy.aspx?ln=de
http://www.tecchannel.de/betriebssysteme/1215/

Danach kann und sollte jeder für sich selber entscheiden, ob er es benutzt oder nicht. Falls nicht, muss man aber wenigstens so schlau sein, sich die Updates aus anderen Quellen zu besorgen und zu installieren.

- "Dienst zur Zeitsynchronisation": Wie bereits geschrieben, gleichen unixoide Systeme bereits seit Jahrzehnten ihre Uhren per NTP ab. Bietet Windows ähnlichen Komfort, muss man es abschalten. Warum? Auch dieser Dienst baut von sich aus keine Onlineverbindungen auf.

- "Dienst für Taskplaner deaktivieren: Auch hier ist der Sinn eher zweifelhaft. Eine Sicherheitslücke im Taskplaner ist allerdings inzwischen bekannt und von MS mit einem Patch gestopft worden. Es gibt jedoch einige Softwarepakete wie z.B. Antivirensoftware, die sich auf einen aktivierten Taskplanerdienst verlassen. Aufgekommen ist diese Empfehlung wohl, weil bei laufendem Taskplaner der Port 1025 oft von Online Portscannern als offen gemeldet wird. Dasselbe passiert aber auch, wenn der Dienst beendet ist.

- "Universal Plug and Play (UPnP) Dienst deaktivieren": Das kann man ohne weiteres machen. Man beraubt sich zwar einiger Möglichkeiten zur Remote Steuerung von ICS oder einigen UPnP-fähigen Routern, aber da der Dienst in der Vergangenheit mit einigen Sicherheitslücken aufgefallen ist, kann man das IMHO verschmerzen.

- "Nachrichtendienst deaktivieren": Kann man machen. Hat aber nichts mit Sicherheit zu tun. Damit kneift man nämlich nur die Augen feste zu und hofft, dass der heranrasende Laster dadurch verschwindet und man nicht überfahren wird. Sinnvoller und weitaus sicherer ist es, einfach die in XP enthaltene Firewall auf der Internetverbindung zu aktivieren. Damit werden Zugriffe von außen zuverlässig verhindert. Übrigens ist der Nachrichtendienst bei XP2 SP2 standardmäßig deaktiviert.

- "Firewalldienst/Gemeinsamen Internetzugriff deaktivieren": Hier gehe ich mit dem ersten Teil der Beschreibung konform. Allerdings ist die Schlussfolgerung, nach der eine Anwendungsfirewall wie Kerio der XP eigenen vorzuziehen wäre, leider falsch. Aktuelle

Schadsoftware ist ohne weiteres in der Lage, Personal Firewalls auszuschalten, **wenn der Anwender mit Administrator Rechten angemeldet ist**. Also wäre ein besserer Rat, auf eine Personal Firewall zu verzichten und stattdessen mit eingeschänkten Accounts zu arbeiten. So oder so kann jedoch **keine** Firewall verhindern, dass ein Programm nach Hause telefoniert, wenn es das wirklich will. Stichwort: Tunneling. Der einzige sichere Schutz davor besteht darin, sich keine "Phone Home" Software zu installieren.

- "Deaktivieren des Security Center Dienstes": Wie der Autor selber schreibt: kann man machen, muss man nicht. Für viele Anwender, die bislang sehr sorglos mit Rechnersicherheit umgingen, ist das Teil IMHO jedoch durchaus sinnvoll.

Der Microsoft Messenger

Dieser Punkt bietet inzwischen nur noch die Deinstallation des Messengers an. Das kann man am schnellsten und nachhaltigsten ohne XP Antispy per Start-->Ausführen--> RunDll32 advpack.dll,LaunchINFSection %windir%\INF\msmsgs.inf,BLC.Remove erreichen.

DLL Dateien deregistrieren

Zum Schluss bietet XP-Antispy noch an, einige DLL Dateien zu deregistrieren. Das sind die Funktionen, mit denen sich viele unbedarfte XP Besitzer dann sehr elegant ins Knie schießen Harmlos ist allerdings „ZIP-Funktionalität deaktivieren“, wenngleich das die meisten aktuellen Packprogramme bei der Installation von sich aus erledigen. Die beiden anderen haben es dafür aber in sich:

- Der Fachpresse folgend wird nach der Installation XP-Antispy installiert und weil man sowieso nicht versteht, was das Programm tut, klickt man halt alles mal an. Und natürlich ignoriert man die Hinweise, die der Autor des Programms zu jeder der Funktionen anbietet. Und nach 30 Tagen kann man sein frisch installiertes XP nicht mehr benutzen, weil man vergessen hat, es zu aktivieren und durch das Setzen von RegDone die Erinnerung daran unterdrückt wurde. Käme man noch in Windows und wollte man es jetzt aktivieren, scheitert dies, weil die dafür erforderlichen DLLs deregistriert wurden. Viel Spaß bei der jetzt fälligen Neuinstallation.

- Oder, auch sehr schön: Das Service Pack1 lässt sich nicht installieren. Ursache? Ebenjene deregistrierten DLLs

- Größere Hardwareveränderungen wurden durchgeführt. XP will erneut aktiviert werden. Es passiert was? Richtig: Es geht nicht. Nach drei Tagen steht dann die Neuinstallation an, weil man sich nicht einmal mehr anmelden kann.

Wer sich auskennt, weiß das natürlich und weiß auch, wie er das Problem umgehen kann. Aber: Wer sich auskennt, deregistriert diese DLLs erst gar nicht. Warum auch? Weil sie für die Aktivierung benötigt werden und die Aktivierung per se etwas Böses ist? Und warum deregistrieren, wenn XP bereits aktiviert wurde? Nein, tut mir Leid, diese Logik erschließt sich mir beim besten Willen nicht. Es gibt nicht den Hauch eines Beweises, dass diese beiden DLLs für irgendetwas außer der Aktivierung genutzt werden oder dass mit ihrer Hilfe Windows ungefragt Daten an MS überträgt.

Fazit und Empfehlungen

Zusammenfassend kann ich also sagen: XP-Antispy ist kein Werkzeug, mit dem man seinen PC sicherer machen kann. Es ist ebenso wenig dazu geeignet, unerwünschte Datenübertragungen zu unterbinden, obwohl genau das sein Name suggeriert und es auch mit dieser Funktionalität von den meisten Anwendern assoziiert wird.

Es ist natürlich in der Hand eines Anwenders, der wenigstens ansatzweise weiß, was er tut (oder die Tipps des Programmautors zu den einzelnen Funktionen zumindest liest), ein praktisches Tool, um einige wenige Systemeinstellungen zentral zu tätigen., ohne sich in die Tiefen der Registry zu begeben. Ob das die ganzen überflüssigen, irreführenden oder sogar potentiell schädlichen Funktionen drum herum rechtfertigt, sei mal dahingestellt.

Nachdem ich jetzt XP-Antispy so massiv kritisiere, muss ich natürlich auch auf Möglichkeiten hinweisen, wie man tatsächlich ohne diese Pseudosicherheit vorgaukelnde Software zu einem stabilen, sicheren und beherrschbaren System kommt. Dafür habe ich hier ein paar weiterführende Links zusammengetragen.

Linktipps

Detailinfos zur Kommunikation von Windows Professional SP1 mit dem Internet:
Der Einsatz von XP Professional mit Service Pack 1 in einer verwalteten Umgebung: Überwachung der Internetkommunikation
http://www.microsoft.com/germany/ms/technetdatenbank/showArticle.asp?siteid=600049

Wer wissen will, was bei der Aktivierung im Detail passiert und auch, welche Daten bei der Onlineaktivierung übertragen werden, der kann sich hier informieren:
Aktivierung entschlüsselt: http://www.tecchannel.de/betriebssysteme/739/index.html

Online Aktivierung entschlüsselt: http://www.tecchannel.de/betriebssysteme/1215/
Weiter geht es mit einer ausführlichen Sammlung von Informationen zum den Themen Personal Firewall und Rechnersicherheit allgemein:
http://www.linkblock.de

Und eine Seite, die sich mit dem Deaktivieren von Diensten unter Windows beschäftigt und ein sehr sinnvolles und praktisches Tool dafür bereitstellt, mit dessen Verwendung man eine tatsächliche Sicherheit erreicht. Auf jeden Fall sollte man sich intensiv mit den Informationen dort beschäftigen.
http://www.ntsvcfg.de