TRUST IN GERMAN SICHERHEIT

G DATA WHITEPAPER

POTENZIELL UNERWÜNSCHTE PROGRAMME (PUP)

TRUST IN GERMAN SICHERHEIT

INHALT

MOTIVATION

Anbieter von Freeware greifen immer öfter auf ein besonders unangenehmes Geschäftsmodell zurück, um ihre kostenlose Software zu monetarisieren: Mit dem Installationsprogramm werden Software-Produkte von Drittanbietern mehr oder weniger verborgen ausgeliefert. Die Drittanbieter bezahlen für jede erfolgreiche Installation eine Provision an den Freeware-Hersteller, gemeinsame Umsatzquelle sind zum Beispiel die direkte Anzeige von Werbung oder die Erstellung und der Verkauf von Nutzerprofilen für personalisierte Reklame. Sogar seriöse Anbieter wie Adobe koppeln auf ihren Seiten ungefragt Zusatzsoftware als „optionales Angebot" an ihre Produkte. Immerhin ist das hier offensichtlich erkennbar und kann schon vor dem Download deaktiviert werden.

Die ungebrochene weltweite Nachfrage nach kostenloser Software hat ein Millionengeschäft heranwachsen lassen. Leidtragende sind jedoch immer öfter die Anwender, die auf diesem Weg zunehmend aggressive Werbeprogramme, Spyware oder allerlei wirkungslose Software gegen vermeintliche Computerprobleme auf den PC bekommen. Zusammenfassend wird diese Art von Software als „potentiell unerwünschte Programme" („PUP") bezeichnet, weil sie zwar keinen direkten Schaden anrichtet, aber Zeit und Nerven kostet, ohne einen Nutzen zu bringen.

Anbieter unerwünschter Programme stellen Ihre dubiose Tätigkeit als legitimes Geschäftsmodell dar und locken Freeware-Hersteller mit zusätzlichen Umsätzen. (Quelle: Computer-Service-Remscheid.de)

Download-Portale wie CNET/Download.com oder Softonic haben das Unterschieben von potentiell unerwünschten Programmen sogar zum zentralen Inhalt ihrer Geschäftstätigkeit gemacht: Jegliches von dort heruntergeladene Programm wird in einen Installer verpackt, der Zusatzsoftware installiert. Selbst ursprünglich „saubere" Software erhält dadurch in jedem Fall einen blinden Passagier. Andere Webseiten verbergen den Link zum Herunterladen seriöser Programme zwischen zahlreichen „Download"-Schaltflächen für zweifelhafte und/oder nutzlose Software, sodass schnell das falsche Programm auf dem eigenen PC landet. Wer nach einem bestimmten Softwaretitel sucht und dabei wahllos eines der oberen Suchergebnisse bei Google anklickt, kann seinen Browser so innerhalb kürzester Zeit durch einen „Browser Hijacker" mit Toolbars, unbekannte Suchmaschinen und Werbeeinblendungen unbrauchbar machen. Dasselbe passiert bei der achtlosen Installation von Freeware – auch wenn diese von seriösen Download-Seiten oder vom Hersteller heruntergeladen wurde. [1] [2]

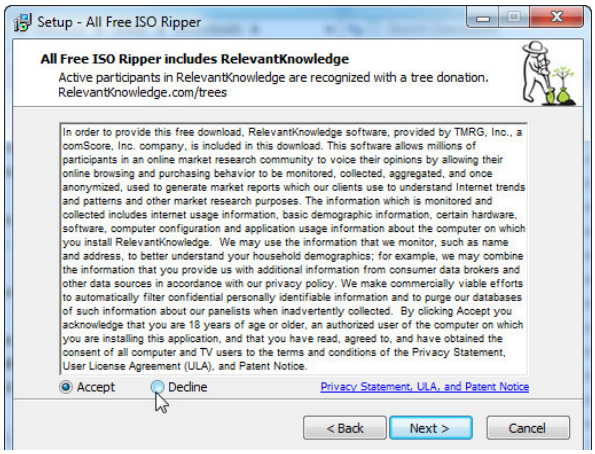
MIT DIESEN TRICKS ERSCHLEICHEN POTENTIELL UNERWÜNSCHTE PROGRAMME IHRE INSTALLATION

Natürlich installiert niemand freiwillig ein Programm auf seinem Computer, das nur einen sehr geringen oder gar keinen Nutzen bietet, dafür aber aggressiv Werbung einblendet oder vorgetäuschte Warnmeldungen anzeigt. Um den Anwender dennoch zu einer Installation zu bewegen, greifen die Anbieter zu unterschiedlichen Methoden:

- Internetseiten werden bewusst so gestaltet, dass die Links zum Herunterladen seriöser Programme zwischen zahllosen auffälligen Download-Schaltflächen für PUP verschwinden. Der Anwender klickt irrtümlich auf eine der Schaltflächen, startet die vermeintliche Installation des gewünschten Programms und erhält stattdessen eine unerwünschte Software.
- Internetseiten zeigen aggressive Werbung an, die vor einem Virenbefall, Registry-Fehlern oder „320 erkannten PC-Problemen“ warnt. Geht der Anwender der Warnung nach, installiert er dabei ein nutzloses Programm, das erst in der kostenpflichtigen „Vollversion“ verspricht, diese vorgeblichen Probleme zu beseitigen.
- Am weitesten verbreitet ist die eingangs beschriebene Bündelung mit seriöser Freeware. Verschiedene Methoden sollen sicherstellen, dass der Anwender bei der Installation die enthaltenen unerwünschten Programme übersieht oder den Eindruck bekommt, dass deren Installation unvermeidbar ist.

Das Arsenal der Tricks, um bei einer Freeware-Installation den Anwender zu übertölpeln und ihm das potentiell unerwünschte Programm unterzuschieben, ist breit gefächert: [3]

- Die potentiell unerwünschte Software wird installiert, wenn der Anwender unaufmerksam ist und die aktivierte Option zur Auswahl der Installation nicht deaktiviert.
- Die Anzeige des potentiell unerwünschten Programms wird in den „benutzerdefinierten“ oder „fortgeschrittenen“ Optionen der Installation versteckt. Nutzt der Anwender die „Express“- oder „empfohlene“ Installation, bekommt er von dem blinden Passagier nichts mit.
- Die Installation des potentiell unerwünschten Programms wird als Annahme der Lizenzbedingungen der eigentlichen Freeware getarnt, lediglich die Abweichung des Programmnamens im Kleingedruckten gibt einen Hinweis. Um die Installation zu verweigern, ist die Ablehnung der Lizenzbedingungen erforderlich. Für den Anwender sieht es jedoch oberflächlich betrachtet so aus, als würde er damit den gesamten Vorgang abbrechen.



Die Installation des unerwünschten Zusatzprogramms wird als Lizenzannahme der Freeware getarnt. (Quelle: pcworld.com)

- Die Option zum Abwählen des potentiell unerwünschten Programms ist grau eingefärbt, sodass sie deaktiviert erscheint. In Wirklichkeit ist sie jedoch anwählbar. Damit soll der Anwender davon überzeugt werden, dass er keine Wahl hat und das Programm mit der Freeware installieren muss.

Die Option zum Ablehnen der Lizenzbedingungen oder der Installation ist grau eingefärbt und scheinbar deaktiviert, obwohl sie sich nutzen lässt. (Quelle: pcworld.com)

- Die Formulierung der Installations-Optionen ist durch doppelte Verneinung bewusst irreführend gestaltet. Die vermeintliche Deaktivierung des potentiell unerwünschten Programms stößt dadurch bei genauerem Durchlesen erst dessen Installation an.

STELLEN POTENTIELL UNERWÜNSCHTE PROGRAMME EINE BEDROHUNG DAR?

Im Gegensatz zu echten Schadprogrammen besitzen PUP keine direkte schädliche Wirkung und keinen Mechanismus zur Weiterverbreitung. Sie stehlen keine Kontodaten, manipulieren keine Bank-Webseiten und infizieren keine Dateien. Zudem werden sie vom Anwender selbst installiert, obwohl dieser oft nichts davon merkt. Vor diesem Hintergrund stufen die meisten Sicherheitslösungen PUP trotz ihrer enormen Lästigkeit nicht als Schadprogramm ein. Das hat nicht zuletzt rechtliche Gründe: Falls ein Programm offenbar keinen direkt Schaden anrichtet, würde die Warnung durch ein Sicherheitsprogramm das Geschäftsinteresse des Anbieters verletzen.

Es ist dennoch möglich, dass dem Anwender durch unerwünschte Programme auf indirektem Weg Schaden entsteht. Denkbar sind zum Beispiel folgende Auswirkungen:

- Durch das Umleiten von Suchanfragen auf unseriöse Suchmaschinen steigt die Gefahr, dass der Anwender auf betrügerische oder mit Schadsoftware manipulierte Webseiten gerät.
- Das ungewollte Anklicken unseriöser und aggressiver Werbung leitet die Installation weiterer unerwünschter Programme oder Schadprogramme ein.
- Die Beseitigung vorgetäuschter Computerprobleme oder Vireninfektionen gegen Bezahlung richtet finanziellen Schaden an, auch wenn der Anwender die Summe freiwillig bezahlt.
- Die Blockierung oder Deaktivierung von Sicherheitsfunktionen im Browser kann Sicherheitslücken für echte Schadprogramme öffnen.
- Funktionen zum Nachladen weiterer Programmteile eröffnen mögliche Sicherheitslücken, über die Schadprogramme auf den Computer gelangen oder Hacker Zugriff bekommen können.

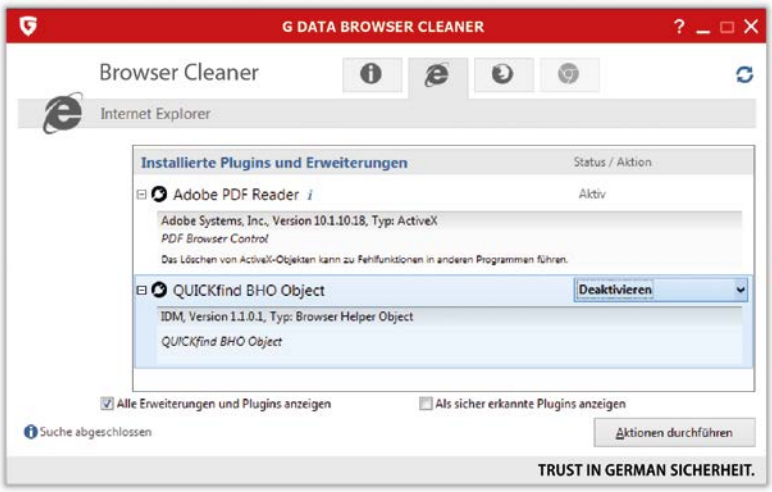
PUP sind also mehr als nur eine lästige Randerscheinung, sondern eine potentielle Gefährdung des Computers.

SO HELFEN G DATA BROWSER CLEANER UND FAKEAVCLEANER DABEI, PUP WIEDER LOSZUWERDEN

So schnell PUP aus Versehen auf dem PC installiert sind, so schwierig sind sie zum Teil wieder loszuwerden. Viele der Anbieter bedienen sich geradezu krimineller Programmiertechniken, um ihre Produkte tief im System zu verankern. [4] Die Deinstallation über die Windows-Systemsteuerung ist in der Regel schwierig und von Laien kaum mit Erfolg durchzuführen. So erfordert der berühmt-berüchtigte Browser-Hijacker „Snap.do“ für jeden Browser eine separate Deinstallation. Andere PUP sind in mehreren Teilen installiert, die vor dem nächsten Systemstart komplett entfernt sein müssen, weil sie sich ansonsten gegenseitig neu installieren.

Selbst erfahrene Anwender können sich die Arbeit durch den Einsatz von G DATA BROWSER CLEANER und G DATA FakeAVCleaner „System Tool“ erheblich erleichtern:

G DATA BROWSER CLEANER arbeitet mit Microsoft Internet Explorer, Mozilla Firefox und Google Chrome zusammen und ermöglicht eine spielend leichte Verwaltung aller installierten Browser-Erweiterungen. Mit einem Mausklick lassen sich alle Plug-ins in der Liste deaktivieren oder entfernen, um den Browser von unerwünschten Erweiterungen zu befreien. Das Tool zeigt per Option alle als sicher eingestuften Plug-ins an, um sie schnell und leicht von unsicheren oder unerwünschten Erweiterungen unterscheiden zu können. G DATA BROWSER CLEANER ist in der umfassenden Sicherheitslösung G DATA TOTAL PROTECTION enthalten und steht dessen Nutzern immer zur Verfügung. Alle anderen Anwender können das Tool kostenlos herunterladen.



Ein Mausklick genügt, um unerwünschte Browser-Erweiterungen aus Firefox, Internet Explorer oder Chrome zu entfernen.

G DATA FakeAVCleaner „System Tool“ entfernt Fake-AV-Tools, die eine Vireninfektion vortäuschen, den Anwender ängstigen und die Gefahr gegen Zahlung einer Gebühr angeblich wieder beseitigen. Zu dieser Kategorie von Programmen zählen auch PUP wie „Reimage Repair“, die anstatt einer Vireninfektion PC-Probleme vortäuschen. G DATA FakeAVCleaner „System Tool“ kann unter https://www.gdata.de/kundenservice/downloads/tools von allen Anwendern kostenlos heruntergeladen werden.

LITERATURVERZEICHNIS

1. G DATA SecurityBlog: „Potentiell unerwünschte Programme: Mehr als nur nervig“ https://blog.gdata.de/artikel/potentiell-unerwuenschte-programme-viel-mehr-als-nur-nervig
2. Peter Stelzel-Morawietz: „Huckepack-Software: Weg mit dem Müll!“ http://www.pcwelt.de/ratgeber/Huckepack-Software-_Weg-mit-dem-Muell-7938592.html
3. How to spot and avoid installing potentially unwanted programs http://www.pcworld.com/article/2429418/how-to-spot-and-avoid-installing-potentially-unwanted-programs.html
4. Jérôme Segura: Potentially Unwanted Program borrows tricks from malware authors https://blog.malwarebytes.org/fraud-scam/2014/12/potentially-unwanted-program-borrows-tricks-from-malware-authors/