Virenscanner - Die zwei Seiten der Medaille

Russland greift die Ukraine an, bedroht den Westen – und plötzlich sind auch russische Virenscanner im Verdacht, durch die russische Regierung für digitale kriegerische Aktivitäten missbraucht zu werden. Das ist das Bild, das sich durch die in den Medien öffentlichkeitswirksam verbreiteten Warnungen im Kopf vieler Menschen ergibt. Was ist denn da eigentlich los? Und stimmt das wirklich? Wir bieten Ihnen einen ruhigen Blick auf die Situation, erläutern in verständlicher Sprache die Hintergründe für solche Warnmeldungen und geben unsere Einschätzung ab.

Das BSI warnt: So begann alles

Das BSI ist das “Bundesamt für Sicherheit in der Informationstechnik”. Es ist die Sicherheitsbehörde des deutschen Staates, die salopp gesagt das Internet schützen soll. Es soll den deutschen Staat, die Wirtschaft, die Gesellschaft und alle Bürger vor digitalen Großgefahren schützen. Aufgrund der politischen Lage sieht das BSI eine relevante Gefahr, dass der Virenscanner “Kaspersky” mit seinem Firmensitz in Russland durch die russische Staatsregierung missbraucht werden könnte, um andere westliche Staaten und Deutschland (darunter vor allem Unternehmen) digital zu gefährden. Weil das BSI eine wichtige, seriöse und unabhängige Behörde ist, wurden die Warnmeldungen schnell in den Medien verbreitet. Das führte zu einer Verunsicherung bei den Menschen, was zu tun ist und wie ernst die Lage wohl sei.

Bundesamt für Sicherheit in der Informationstechnik

Alle Virenscanner sind ein Problem

Doch was steckt dahinter? Ist denn die grundsätzliche Gefahr wirklich real? Kann ein Virenscanner derart missbraucht werden? Immerhin ist doch der Zweck des Virenscanners, Gefahren abzuwehren! Will man hier vielleicht einfach nur das russische Unternehmen Kaspersky unter einem Vorwand wirtschaftlich “sanktionieren”?

Eines steht fest, ist unbestritten und eindeutig:

Ein Virenscanner kann sehr leicht und mit wenig Vorbereitungszeit von einem Beschützerprogramm in ein Angriffsprogramm umgewandelt werden. Jeder (!) Virenscanner erhält durch die Installation einen tiefgehenden Zugriff auf das Betriebssystem, darf (teilweise sogar vollautomatisch) Dateien ändern, löschen, öffnen etc. Es ist, als würde man einem Sicherheitsmann, der das eigene Haus beschützen soll, alle Haustürschlüssel überreichen.

Würde sich der Sicherheitsmann bzw. der Virenscanner entschließen, den Haushalt nicht mehr zu beschützen, wäre der Hausbesitzer ihm vollends ausgeliefert. Er könnte aktiv das Haus bzw. den Computer gefährden oder aber “wegschauen”, wenn ein Krimineller bzw. ein Schadprogramm angreift. Natürlich geht man davon aus, dass das Verhältnis von Hausbesitzer und Sicherheitsmann bzw. von Computernutzer und Virenscannerhersteller keinen solchen Wandel erfährt. Und in der Vergangenheit gab es keine Beweise, dass dies schon einmal bei einem Virenscanner geschehen ist. Aber: die Theorie dafür existiert und man könnte das sehr leicht und schnell in die Praxis umzusetzen.

Halten wir als 1. Fazit fest:

Sobald man einen Virenscanner nutzt, ist auf dem Computer ein Programm installiert, das aufgrund seiner tiefgreifenden Berechtigungen den Computer schützen kann – oder aber die

identischen Berechtigungen verwenden kann, um den Computer zu gefährden. Zumindest in der Theorie, denn in der Praxis ist diese Gefährdung ein Ereignis, das noch nicht vorkam.

Andere Zeiten, andere Bösewichte
Der theoretische Missbrauch eines Virenscanners durch den Staat, in dem der Virenscannerhersteller seinen Firmensitz hat, ist durch Regierungsgewalt also theoretisch denkbar und schnell durchführbar. Aktuell, daher die BSI-Warnung, würde man der russischen Regierung aufgrund des Angriffs auf die Ukraine einen solchen Schritt zumuten, wenn auch mit keiner Beweislage und keiner großen Wahrscheinlichkeit. In anderen Zeiten kam die "Bedrohung" von anderer Seite und die Experten befürchteten einen identischen Missbrauch von anderer Stelle: Die US-amerikanische Verfolgung internationaler Terroristen und die NSA-Skandale ließen US-amerikanische Virenscanner in den Verdacht geraten und als die deutsche Bundesregierung einen "Staatstrojaner" plante, war die Befürchtung, dass die deutschen Virenscanner "wegschauen" sollten, damit der Staatstrojaner unbemerkt seinen Dienst tun kann.

Halten wir als 2. Fazit fest:
Das Problem ist die Technik und nicht die aktuelle politische Lage oder die Befürchtungen der Menschen, wer "angreifen" könnte. Je nach Szenario ändert sich der vermutete potentielle Akteur, aber die Grundlage, aufgrund dessen ein solcher Missbrauch möglich wäre, existiert bei allen Virenscannern von allen Herstellern. Es liegt in der Technik begründet, es ist die "Natur eines Virenscanners".

Was soll ich denn jetzt machen?
Das ist wohl die Frage, auf die es letztendlich hinausläuft. Wenn sich ein Virenscanner so schnell "gegen mich wenden" kann, warum soll ich denn dann überhaupt einen verwenden? Welcher Virenscanner bietet die geringste Chance, derart missbraucht zu werden?

Unsere Empfehlung ist seit Jahren:
Die oben beschriebenen grundlegenden Hintergründe sorgen dafür, dass quasi jeder Virenscanner, der installiert wird, theoretisch ein Problem sein kann. Daher ist unsere Empfehlung, den beim Windows-Betriebssystem integrierten **Windows Defender** zu verwenden. Er ist kostenfrei und werbefrei und somit bereits, unabhängig von den hier besprochenen theoretischen Szenarien, ein empfehlenswerter Virenscanner. Denn ein ganz anderer Aspekt ist, dass Virenscanner nicht selten ordentliche Geldbeträge kosten. Zwar gibt es oft auch eine kostenfreie Variante des gleichen Virenscanners. Aber in dieser kostenfreien Variante wird viel verwirrende Werbung eingeblendet, die dem Anwender das Gefühl vermitteln, er müsse sehr wohl die kostenpflichtige Version kaufen. Der Windows Defender ist also auch deswegen empfehlenswert, weil er kostenfrei ist und keine Werbung für eine kostenpflichtige Version enthält. Der Windows Defender springt außerdem **automatisch** an, wenn kein anderer Virenscanner installiert ist. Wenn Sie also bisher einen anderen Virenscanner besitzen und diesen löschen (eine simple Deinstallation reicht aus, um den Virenscanner zu löschen), dann übernimmt der Windows Defender sofort seinen Schutzdienst.

Der Gedanke hierbei ist folgender:
Das Windowssystem stammt bekanntlich aus der Schmiede von Microsoft. Damit hat Microsoft als Hersteller sowieso gewissermaßen "einen Schlüssel für Ihr Haus". Der Hersteller des Betriebssystems hat natürlich die gleichen "systemweiten Rechte", die auch ein Virenscanner hat. Das lässt sich nicht vermeiden. Daran kann man nur etwas ändern, wenn man ein anderes Betriebssystem wie Apple oder Linux verwenden würde, und auch dort wären die Situationen ganz ähnlich. Denn wer ein Betriebssystem programmiert hat, ist entsprechend in der Lage, auf alle Bereiche Zugriff zu nehmen. Auch hier ist das nur ein theoretisches Szenario, es gibt keine Beweise und keine Befürchtungen, dass Microsoft etwas Derartiges tun würde und je tat. Ein wenig Vertrauen darf man also durchaus in Microsoft und die Virenscannerhersteller setzen, dass sie sich nicht so leicht durch einen Staat beeinflussen lassen. Wenn man aber einen Virenscanner

eines anderen Herstellers installiert, dann hat man zwei potentielle Hersteller (Microsoft und der Virenscannerhersteller), die theoretisch auf den Computer zugreifen könnten. Wenn man aber einen Virenscanner von Microsoft verwendet, ist beides (Virenscanner und Betriebssystem) vom gleichen Hersteller und man halbiert das Risiko. So einfach ist der Hintergrundgedanke.

Virenscanner leisten keine schlechte Arbeit
Das Problem, auf das wir in der aktuellen Lage und der BSI-Warnung nun alle aufmerksam wurden, ist also nicht, dass ein Virenscanner schlechte Arbeit erledigen würde oder dass einige Virenscanner von Grund auf schlecht in der Erkennung von Schadprogrammen seien und daher nicht mehr genutzt werden sollen. Im Gegenteil: Alle auf dem Markt befindlichen Virenscanner schützen den Computer aktuell sehr gut vor Schadprogrammen, sie sind allesamt von sehr guter Qualität. Das Problem ist vielmehr, dass ein theoretisches Szenario möglich wäre, in dem ein Virenscanner durch eine Regierung missbraucht werden könnte.

An alle Kaspersky-Nutzer*innen:
Einige Menschen, die den Kaspersky gekauft haben und seit Jahren nutzen und zufrieden sind, fragen sich, warum der Virenscanner plötzlich “nicht mehr gut sein soll”. Immerhin schneidet er seit Jahren sehr gut in allen Tests ab und hat sich einen Ruf erarbeitet, einer der besten Virenscanner zu sein. Diese Frage geht am Problem vorbei. Der Kaspersky ist ein guter Virenscanner! Wenn eine Regierung aber einen Virenscanner umprogrammieren lassen würde, um einen digitalen Cyberangriff durchführen zu können, spielt die Qualität und der Ruf eines Herstellers keine Rolle.

An alle Smartphone-Nutzer*innen:
Auch auf den Smartphones wird immer häufiger zu einem Virenscanner gegriffen. Wie in der Windows-Welt, gibt es auch auf den Smartphones ab Werk integrierte Sicherheitssysteme, die das Gerät automatisch schützen. Die Installation eines zusätzlichen Schutzprogramms kann aber eine sinnvolle Sache sein. Wir haben für die Smartphone-Welt und die Frage nach einem passenden Virenscanner einen aktuellen Erklärfilm erstellt. Er ist für alle Newsletter-Leser kostenfrei. *(Siehe unten am Ende des Beitrags.)*

Fazit
Die aktuelle politische Lage hat das grundlegende Problem der Virenscanner auf einen Hersteller fokussiert: Kaspersky. Schuld daran ist nicht Kaspersky und auch nicht Russland, sondern die “Natur eines Virenscanners”, die einen theoretischen Missbrauch möglich macht. Einen Beweis oder eine hohe Wahrscheinlichkeit existiert weder für den aktuellen russischen Fall noch für frühere Fälle. Und es sieht auch nicht danach aus, als gäbe es in Zukunft wahrscheinliche Szenarien, in denen ein solcher Missbrauch geschieht. Um trotzdem auf Nummer Sicher zu gehen, ist die Nutzung des Microsoft-eigenen Virenscanners “Windows Defender” eine Option, das sehr kleine Risiko weiter zu reduzieren.

Zusatzhinweis für Apple und Linux:
Wie so oft, sind auch in dem aktuellen Szenario diese beiden Betriebssysteme weniger stark gefährdet. Das ist auch der Grund, warum der Erklärfilm “Virenscanner auf dem Smartphone” nur für Android gedacht ist: Apple iPhones benötigen keinen Virenscanner.

Unsere passenden Filme für Alle (auch Nicht-Mitglieder):

Wie lösche ich ein Programm, *Video-Player, 00:00 – 06:02*
Wie nutze ich den Windows Defender, *Video-Player, 00:00 - 02:43*
Virenscanner für das Smartphone (Android), *Video-Player, 00:00 - 06:06*

Quelle: https://levato.de/virenscanner-die-zwei-seiten-der-medaille/