# Offener Brief an die Stiftung Warentest

Sehr geehrte Damen und Herren,

In ihrer Ausgabe 4/12 betrachtet die Stiftung Warentest Sicherheitssoftware. Dabei wurden insgesamt 18 Antiviren- und Internetsicherheitsprodukte getestet. Als Verbraucher schätzen wir die Arbeit der Stiftung Warentest als Testgremium auch wegen ihrer Unabhängigkeit überaus. Um so mehr wundern wir uns, dass die Testmethoden leider nur unzureichend beschrieben sind. So ergibt sich der Eindruck, dass der Schwerpunkt auf veraltete Testmethoden gelegt wurde, die vor einigen Jahren absolut valide waren – es heute aber leider nicht mehr sind. Jedoch scheint diese Methode weder die Funktionsweise moderner Sicherheitssoftware innerhalb der getesteten Programme zu prüfen noch das Verhalten der Benutzer oder tatsächlicher Infektionen abzubilden. Herstellerübergreifend und zusammen mit unabhängigen Softwaretestern bieten wir Ihnen deshalb eine offene Diskussion über Ihre Testmethoden an und hoffen, Ihnen dabei einige Anregungen geben zu können, um zukünftig realitätsnähere Testergebnisse erzielen zu können.

Wie Sie sicher wissen, gibt es auch schon kritische Kommentare Ihrer Leser auf Ihrer Webseite, die auch nicht in ihrem Sinne sein können (https://www.test.de/themen/computer-telefon/test/Schadprogramme-Angriff-aus-dem-Internet-4348485-4348487/).

Mit ZDNet hat zudem auch ein führendes deutsches IT-Onlinemedium das Thema bereits kritisch aufgegriffen: http://www.zdnet.de/news/41561250/stiftung-warentest-findet-nur-vier-von-18-antiviren-programmen-gut.htm

Vor diesem Hintergrund fragen wir uns, warum die Stiftung Warentest nicht von Beginn an mit etablierten Testinstituten in diesem Bereich zusammengearbeitet hat, die auf eine moderne Testmethodik setzen, um die tatsächliche Gefährdungslage für Nutzer und die Leistung der Schutzsoftware in einem realistischen Szenario abzuprüfen und diese auch vergleichbar zu machen. Auch die Anti Malware Testing Standards Organization hat grundlegende Empfehlungen veröffentlicht, um Testern dabei zu helfen, Aufbau und Durchführung Ihrer Tests zu optimieren. Unser Eindruck ist, dass diese in ihrem Test nicht berücksichtigt wurden.

**Besonders folgende Aspekte der Testmethoden der Stiftung Warentest müssen wir leider hinterfragen:**

Die verwendeten Methoden **prüfen im Schwerpunkt die reaktive signaturbasierte Erkennung von inaktivem Schadcode ab,** anstelle von **praxisnahen Tests**, die alle vorhandenen Schutz-und Erkennungstechnologien (z.B. verhaltensbasierte Erkennung) mit einschließen und auf die Hauptinfektionswege (Internetseiten mit aktivem Schadcode, z.B. Drive-by) fokussieren.

Es macht heutzutage keinen Sinn mehr, Sicherheitsprodukte zum Teil ohne Internetverbindung zu testen. Die Hauptinfektionsquelle ist das Internet und Malware benötigt das Internet, um Schaden anzurichten. Ein Hauptzweck von Malware, wie von Ihnen auch im Artikel beschrieben, ist das Stehlen von Daten, diese müssen allerdings über das Internet übertragen werden. Das Beispiel mit einem USB-Stick ist demnach zwar valide, was die Infektion an sich angeht, aber der echte Schaden könnte abgewendet werden, da die Schutzprodukte die Schadfunktion stoppen würden, sobald eine Internetverbindung besteht. Würde man den Schädling von dem USB-Stick ausführen oder nach dem Kopieren auf die Maschine starten würde man feststellen, ob andere Schutzmethoden wie die verhaltensbasierte Erkennung greifen. Selbst ein Programm ohne eine einzige Signatur könnte in der Realität einen sehr guten Schutz bieten, indem dynamische Erkennung oder Reputationsprüfung genutzt wird. Dies wird in Ihrem Test aber nicht berücksichtigt.

Zudem mahnt ihr Test die langsamen Updates der Virensignaturen an und weist darauf hin, dass bei einigen Herstellern die Updatefrequenz nicht eingestellt werden kann. Dies ist bei Cloud-basierenden Reputations-Dienstleistungen obsolet, da diese Arbeit in der Wolke gemacht wird – bei bestehender Internetverbindung. Die Wolke wird also ständig aktualisiert, so dass die Notwendigkeit für Updates auf dem Client entfällt.

**Für mehr Transparenz: Unser Angebot zur offenen Diskussion**

Die Stiftung Warentest erwähnt in der Testbeschreibung nicht, wie aktive Malware und Drive-By-Downloads getestet wurden. Auch die die näheren Beschreibungen die nach der Testveröffentlichung online von Ihnen veröffentlicht wurden, werfen leider weitere Fragen auf

Deshalb würden wir gerne einige weitere Themen mit Ihnen diskutieren:

- Was waren die Quellen der Samples? Wie hat die Stiftung Warentest sichergestellt, dass es sich tatsächlich um Malware handelt?
- Wurde nur die Erkennung über Signaturen oder wurde auch der Schutz getestet (was passiert bei Ausführung des Schadprogrammes, wird auch wirklich alles geblockt)?
- Wurden keinerlei Reparatur – oder Systemwiederherstellungstests durchgeführt? Wie gut helfen die Produkte bei einer Infektion?
- Es scheint einen einseitigen Fokus auf Signaturen zu geben. Was ist mit dynamischer Erkennung oder Reputationsprüfung?

- Warum wurden keine Fehlalarm-Tests durchgeführt? Damit sind die Erkennungsraten mit Vorsicht zu genießen. Ein Produkt, das einfach alles erkennt (sowohl gutartige als auch bösartige Dateien), hätte in Ihrem Test – soweit wir ihn momentan verstehen – hervorragend abgeschnitten, wäre aber in der Realität nicht zu gebrauchen.
- Warum lief der Test auf virtuellen Maschinen? Das kann die Ergebnisse verfälschen, da digitale Schädlinge auf virtuellen Maschinen anders reagieren können bzw. nicht oder nicht richtig funktionieren, so dass auch keine erkennungswürdige Schadfunktion vorliegt.

**Anerkannte Teststandards**

Europaweit renommierte Labors für das Testen von Sicherheitssoftware arbeiten heute nach folgenden Standards:

Alle Samples werden live aus dem Internet geladen – zeitnah zum Test (maximal 24 Stunden alt). Alle Samples werden zeitgleich mit allen Produkten getestet. Die Samples werden ausgeführt. Alle Sicherheitskomponenten innerhalb eines Produkts werden getestet, um die Effektivität des Gesamtpakets aufzuzeigen. Es wird das Angriffsszenario und nicht ein einzelnes Produktfeature abgekoppelt vom Gesamtpaket getestet. So stellt man sicher, dass man keine Produkte benachteiligt, die ein bestimmtes Feature nicht haben, aber in der gleichen Situation trotzdem mit einer anderen Technologie schützen. Bei über 70.000 neuen Schädlingen pro Tag ist Signaturerkennung nur noch eines von mehreren Mitteln, die zur Verfügung stehen – es müssen alle Funktionen eines Sicherheitsprodukts überprüft werden.

Leider fehlt bei Ihrem Test eine detaillierte Beschreibung der Methoden, die uns helfen würde, Ihr Vorgehen besser zu verstehen. So könnten wir auch besser nachvollziehen, warum Sie ein bestimmtes Angriffsszenario zur Bewertung der Produkte gewählt haben. Dann lassen sich die Resultate richtig bewerten – aus unserer Sicht, aber vor allem auch aus Sicht der Verbraucher.

Derzeit haben wir den Eindruck, dass Ihre Veröffentlichung bei Verbrauchern und Nutzern unserer Produkte zu einer gewissen Verunsicherung führt, die aus unserer Sicht nicht notwendig ist.

Um diese Punkte unparteiisch und transparent mit Ihnen zu besprechen und anschließend eventuell auch wissenschaftlich überprüfen zu lassen, schlagen wir vor, die Testmethodik und die verwendeten Samples unter Einbeziehung einer unabhängigen und unbeteiligten Stelle zu diskutieren.
Hierfür hat sich mit der AV-TEST GmbH eines der renommiertesten Testinstitute Europas bereit erklärt, entweder im Labor der Stiftung Warentest oder in den Geschäftsräumen des AV-TEST-Instituts.

Zudem ersuchen wir die Stiftung Warentest nachdrücklich, in ihrer nächsten Ausgabe an hervorgehobener Stelle darauf hinzuweisen, dass sie mit uns diese Punkte diskutieren, und ihre Leser zu informieren, dass die verwendeten Testszenarien, die bei vielen Produkten zu schwachen Ergebnissen geführt haben, in Alltagssituationen nicht auftreten. Zudem bitten wir Sie, einen herstellerübergreifenden Dialog mit uns aufzunehmen, um künftig die Alltagssituation Ihrer Leser in Ihren Tests besser abbilden zu können.

Mit freundlichen Grüssen

Claus Meisel, Checkpoint

Klaus Jetter, F-Secure

Josef Pichlmayr, Ikarus

Magnus Kalkuhl, Kaspersky Lab

Toralv Dirro, McAfee

Markus Mertes, Panda Security

Stefan Wesche, Symantec

Raimund Genes, Trend Micro

Andreas Marx, AV-Test