G Data

Whitepaper 01/2011

# Das Duell: Kostenlose gegen kostenpflichtige Security-Software

Eddie Willems
G Data Security Evangelist



Geschützt. Geschützter. **G Data.**

# Inhalt

# 1. Einführung

Kostenlose Antiviren-Software liegt voll im Trend und erfreut sich großer Beliebtheit. Eine Studie von Opswat belegt, daß jeder zweite Computer auf der Welt von kostenloser Antiviren-Software geschützt wird[1]. Tatsächlich ist die Frage ja auch berechtigt, warum man für Antiviren-Software Geld bezahlen soll, wenn es auch kostenlose Alternativen gibt.

Dieses Whitepaper versucht zu erklären, was kostenlose AV-Software leistet – und was nicht. Es durchleuchtet die „Hintergegdanken" der Hersteller für kostenlose Software und gibt Hilfestellungen für die richtige Auswahl von Sicherheitslösungen.

# 2. Kostenlos kostet viel – nämlich viel Know-how.

Eine Binsenweisheit lautet: „Einem geschenktem Gaul schaut man nicht ins Maul". Damit ist trefflich gemeint, daß man sich bei kostenlosen Lösungen gewisser Abstriche oder Unzulänglichkeiten bewusst sein sollte. Computernutzer, die die Grenzen ihrer Free-AV Lösung kennen und sie mit geeigneten Zusatztools ergänzen, können Geld sparen. Allerdings ist dazu eine Menge Know-how erforderlich, das üblicherweise nur Security-Profis zur Verfügung steht. Wer sich ausschließlich auf seine kostenlose Antiviren-Software verlässt, geht mitunter erhebliche Risiken ein!

## 2.1. Was leistet kostenlose Antiviren-Software? Und was nicht?

Die am Markt befindlichen kostenlosen Antiviren-Lösungen zeigen in Vergleichstests von Computermagazinen recht hohe Erkennungsraten bekannter Schädlinge und schneiden daher oft gut ab.

Andererseits sollte eine moderne Security-Software die Einfallstore für Malware abriegeln. Das sind, Webseiten, E-Mails oder offene Ports von Chat-Programmen, Downloadern usw.. Dagegen schützen Schutztechnologiene wie AntiSpam, Webfilter, Firewall, verhaltensbasierte Erkennung und Cloud Security, Genau das fehlt bei kostenloser Antiviren-Software in der Regel:

*Tabelle 2.1.: Gegenüberstellung der Sicherheits-Leistung von kostenloser und kostenpflichtiger AV*

| **Feature** | **Kostenlose AV** | **Kostenpflichtige AV** |
|---|---|---|
| Webschutz (http-Filter) | ✗ | ✓ |
| Antiphishing | ✗ | ✓ |
| Cloud Security | ✗ | ✓ |
| Firewall gegen Hacker Angriffe | ✗ | ✓ |
| Spam und E-Mail Filter | ✗ | ✓ |

Fatal ist, daß Geschäfts- und Abwicklungsprozesse zunehmend ins Internet ausgelagert werden. Daher konzentrieren sich Spam- und Phishing-Attacken zusehends auf Web 2.0 Plattformen und soziale Netzwerke und verzichten mehr und mehr darauf, Code auf dem Computer zu speichern, um stattdessen wertvolle Daten direkt online zu stehlen.

[1] *http://www.oesisok.com/news-resources/reports/worldwide-antivirus-market-share-report%202010*

Und genau dagegen ist kostenlose Antiviren-Software machtlos, weil weder der Mailverkehr, noch der http-Traffic überwacht wird.

Im nachfolgenden Beispiel versuchten Kriminelle, über eine Phishing-Attacke auf Facebook[1] Accountdaten zu stehlen:


***Screenshot 1:*** *Phishing-Attacke im Facebook*

Dabei sollte der Nutzer die Sperrung seines Profils mit einem Klick auf einen Link verhindern. Hinter dem Link verbirgt sich eine Eingabemaske für Benutzername und Passwort. Werden diese Felder ausgefüllt, ist der Account gestohlen und wird für die Verbreitung von Spamnachrichten missbraucht. Einen Schutz vor solchen Angriffen bietet nur eine kostenpflichte Software.

## 2.2. Wie können manche Hersteller überhaupt Antiviren-Software kostenlos anbieten?

Die Entwicklung von Software kostet Geld. Die Software muß programmiert und ausführlich getestet werden und sollte im Idealfall im intensiven Kontakt mit Kunden ständig verbessert und erweitert werden. In kürzester Zeit müssen Signaturen für neue Schädlinge erstellt werden. Dabei dürfen keine Fehler unterlaufen. Dazu braucht man geschulte Spezialisten und modernste Technologie. All das kostet viel Geld. Sind Anbieter von kostenloser AV-Software einfach gute Menschen, die zugunsten ihrer Kunden auf ihren Obolus verzichten?

Keinesfalls. Die Anbieter kostenloser Antiviren-Software verzeichnen im Moment das stärkste Umsatzwachstum der Security-Branche - natürlich mit kostenpflichtiger Software. Das Business Modell basiert auf der massenhaften Verbreitung kostenloser Basis-Versionen und dem

[1] Vgl. Pressemeldung http://www.gdata.de/ueber-g-data/pressecenter/pressemeldungen/pressemeldung/article/1807-trickreiche-facebook-nachricht.html

anschließenden Verkauf kostenpflichtiger Upgrades. Dazu wird mehr oder weniger bewusst auf die unter 1.1 angeschnittenen Sicherheitsmodule verzichtet, die der sicherheitsbewusste Kunde dann dazukaufen kann. So wird Markenbekanntheit und Verbreitung ohne hohe Marketingkosten erreicht. Das Anbieten kostenloser Antiviren-Software ist also eine Art Marketing-Masche, die man als „Freemium" bezeichnet – leider auf Kosten der Kunden, die glauben, mit der Free-AV eine vollwertige Lösung zu besitzen.

**Sparpotential Qualität**

Außer beim Marketing wird bei kostenloser Software auch im Bereich Kundenservice und Qualitätssicherung gespart. So werden immer wieder Fälle bekannt, wo unzureichend getestete Software an Kundengruppen freigegeben wurde. Die Folgen sind Fehlerkennungen und Fehlfunktionen. Die Free AV-Hersteller sehen es gelassen: die Fehlerakzeptanz ist bei Freeware-Kunden nun mal höher als bei kommerziellen Kunden. Denn wer schaut dem geschenkten Gaul schon ins Maul?

**Support? Fehlanzeige.**

Die Freeware-Kunden helfen sogar teilweise kräftig mit: bei Lokalisierungen, Dokumentationen und Hilfestellungen bei Problemen mit der Software. Auf persönliche professionelle Hilfe des Herstellers hofft man vergeblich. Weder per Telefon, noch per Mail wird Kundenservice angeboten. Stattdessen verweisen die Free AV-Hersteller in der Regel auf Online-Hilfequellen wie FAQs und Foren. Hat man sich erst einmal was eingefangen, lässt einen der Hersteller meistens im Regen stehen.

*Tabelle 2.2.: Gegenüberstellung der Service-Leistung von kostenloser und kostenpflichtiger AV*

| Feature | Kostenlose AV | Kostenpflichtige AV |
|---|---|---|
| FAQs | ✓ | ✓ |
| Service-Foren | ✓ | ✓ |
| Telefon-Service | ✗ | ✓ |
| Mail-Service | ✗ | ✓ |
| Fax-Service | ✗ | ✓ |

## 2.3. Wie kann man kostenlose Antiviren-Software zu Rundumschutz-Lösungen erweitern?

Es gibt natürlich die Möglichkeit, eine kostenlose Antiviren-Software mit anderen kostenlosen Tools zu kombinieren (Achtung: hierbei könnten Inkompatibilitäten oder Sicherheitslücken auftreten!). Dazu gehören eine Personal Firewall und ein Spamfilter; den wichtigsten Teil stellt allerdings ein geeigneter Webschutz dar.

**TIPP:** Empfehlenswert als Free AV-Add-on ist das kostenlose Tool **G Data CloudSecurity**, das als Explorer-Plugin kompatibel zu allen Virenscannern ist und keine Performance beim Surfen verbraucht. **G Data CloudSecurity** blockt in Echtzeit in der Cloud Surfer vor infizierten Webseiten und Phishingseiten. Weitere Infos unter: www.free-cloud.com

## 2.4. Was kann kostenpflichtige Security-Software besser?

Kostenpflichtige Security-Software erkennt und entfernt Malware nicht nur zuverlässig, sondern sichert auch alle Einfallstore gegen Angriffe wirkungsvoll ab (siehe Tabelle 2.1.). Und bei kostenpflichtiger Security-Software greifen alle Schutzmechanismen nahtlos ineinander. Die Schutzmodule sind so aufeinander abgestimmt, daß keine Sicherheitslücken übrigbleiben. Im geschilderten Fall der Phishing-Attacke auf Facebook unter 2.1. wird die Zielseite schlicht geblockt.

Die Hersteller kostenpflichtiger Security-Software investieren auch in Qualitätssicherung und meist kostenlosen Kundenservice (siehe Tabelle 2.2.). Der direkte Kundenkontakt und Kundenzufriedenheit werden als wichtig erachtet, um die Security-Lösung zu verbessern und weiterzuentwickeln.

# 3. Fazit

Die Nutzung irgendeiner Antiviren-Lösung – ob kostenlos oder kostenpflichtig – ist besser, als sich ungeschützt ins Internet zu begeben – das weiß heute fast Jeder.

Entscheidet man sich für kostenlose AV-Software, sollte man sich der fehlenden Schutzmechanismen im Klaren sein und den Virenschutz um geeignete Zusatztools ergänzen. Da hierzu neben der Kenntnis der Sicherheitslücken auch noch Probleme durch Inkompatibilitäten und mangelhaftes Ineinandergreifen der Tools auftreten können, empfehlen wir diese Schutzvariante nur professionellen Computer-Nutzern.

Wer sich seiner Sache nicht so sicher ist oder wem die Wartung und Bedienung vieler einzelner Tools zu umständlich ist, sollte besser auf kostenpflichtige Security-Lösungen zurückgreifen, die lückenlos alle Sicherheitsrisiken abdecken, einen nahtlosen Rundum-Schutz gegen moderne Gefahren bieten und obendrein mit gutem Service den Kunden nicht im Regen stehen lassen.