

UNABHÄNGIGE TESTS: REAKTIONSZEIT

Die operative Reaktion der Entwickler von Anti-Viren Programmen auf neue Viren wird zum grundlegenden Kennzeichen der Effektivität des Datenschutzes.

Anfang 2004 grassierten mehrere Epidemien, die in ihrer Zerstörungskraft alles bisher Dagewesene weitaus übertrafen. In diesem Zusammenhang hat eine Forschergruppe der Universität Magdeburg (AV-Test.org) eine unabhängige Evaluation der Reaktionsgeschwindigkeit von Anti-Viren Entwicklern auf neue Codes durchgeführt. Im Rahmen dieser Forschungsarbeit ermittelten die Analytiker den zeitlichen Durchschnittswert zwischen Registrierung eines neuen Virus und der Publikation von Updates der Anti-Viren Dateien. Als Kontrollereignisse wurden Viren ausgewählt, die erst vor kurzem erschienen und mit Hilfe heuristischer Methoden identifiziert wurden. Hierzu gehörten die Programme Dumaru.y, MyDoom.a, Bagle.a and Bagle.b.

Diese Analyse ist objektiver als Vergleichstests von Fachzeitschriften und Forschungszentren. Hier werden oftmals veraltete Viren-Sammlungen verwendet, die bereits Monate zuvor entdeckt wurden. Dabei entgeht dem Anwender bei diesen Tests ein eminent wichtiger Faktor - die operative Reaktionszeit. Gerade dieses Charakteristikum gibt Aufschluss über die Hauptfunktion eines Anti-Viren Programms - den zuverlässigen Schutz gegen neue Viren-Bedrohungen. Die Magdeburger Forschungsergebnisse demonstrieren klar die wirklichen Qualitäten eines Anti-Viren Programms und fixieren somit sein eigentliches IT-Schutzniveau.

Für maximale Analyse-Genauigkeit der Publikations-Intervalle von Anti-Viren Dateien verwendeten die Forscher Script-Programme, die die Server der Anti-Viren-Programme alle 5 Minuten auf neue Updates überprüften. Die Messungen der Reaktionsgeschwindigkeiten ergaben, dass die durchschnittliche Reaktionszeit von Kaspersky Labs auf neue Viren-Bedrohungen am kürzesten ist.

Die Ergebnisse der Forscher aus Magdeburg ergaben folgende Hierarchie nach operativen Reaktionszeiten der führenden Anti-Viren Entwickler.

1. Kaspersky Labs	06:51 h
2. Bitdefender	+ 22 %
3. Virusbuster	+ 28 %
4. F-Secure	+ 33 %
5. F-Prot	+ 35 %
6. RAV	+ 35 %
7. AntiVir	+ 37 %
8. Quickheal	+ 54 %
9. InoculateIT-CA	+ 59 %
10. Ikarus	+ 68 %
11. AVG	+ 75 %
12. Avast	+ 79 %
13. Sophos	+ 81 %
14. Dr. Web	+ 83 %
15. Trend Micro	+ 91 %
16. Norman	+ 92 %
17. Command	+104 %
18. Panda	+105 %
19. Esafe	+152 %
20. A2	+253 %
21. McAfee	+282 %
22. Symantec	+297 %
23. InoculateIT-VET	+335 %

Darüber hinaus erhielten die russischen Entwickler die besten Noten für die kürzesten Intervalle der Publikation von Updates. Anwender von Kaspersky Labs erhalten automatisch alle 3 Stunden, 24 Stunden am Tag Updates der Anti-Viren Dateien und sind somit am besten gegen Viren-Bedrohungen geschützt.

Folgende Statistik zeigt deutlich die Führungsposition von Kaspersky Labs

Intervalle der Updates von Anti-Viren-Dateien
(in alphabetischer Reihenfolge):

Produkt	Anzahl Updates pro Woche
AntiVir (H+BEDV)	5-6
Avast! (Alwil)	2
AVG (Grisoft)	2
BitDefender	3-4
Command	2
Dr.Web	6
eSafe (Aladdin)	5
eTrust (CA)	4-5
F-Prot (Frisk)	4-5
F-Secure	6-7
Ikarus	4
Kaspersky Labs	min. 56
McAfee/NAI	1
Norman	2
Panda	7
Quickheal	4
Sophos	4-5
Symantec	1-2
Trend Micro	2-3
VirusBuster	4-5

Die Führungsposition von Kaspersky Labs konnte maßgeblich durch die Einführung der neuen Technologie 'Rapid Virus Response' ausgebaut werden. Seit Ende Dezember 2003 erhalten die Anwender von Kaspersky Anti-Virus regelmäßig 56 Updates der Anti-Viren Dateien pro Woche, wobei Eil-Updates nicht inbegriffen sind - diese erscheinen gegen Viren mit höchster Gefahrenstufe. Wichtig ist zudem, dass alle regulären Updates von Kaspersky Anti-Virus vor der Publikation eine mehrstufige Test-Prozedur unterlaufen, die Kompatibilität mit unterschiedlichen Betriebssystem und Konfigurationen sichert.

Viele Anti-Viren Entwickler versorgen ihre Anwender mit Beta-Versionen der Updates. Diese werden nicht auf Kompatibilität geprüft und können daher die Leistungsfähigkeit des Anwender-Computers beträchtlich stören. Alles in allem reagiert heute Kaspersky Labs am schnellsten auf neue Viren-Bedrohungen und die Anwender von Kaspersky® Anti-Virus sind jederzeit am besten gegen Viren geschützt.

Details über die Forschungsarbeit finden Sie unter:
http://itmanagement.earthweb.com/columns/executive_tech/article.php/3316511