Gerald Himmelein, Noud van Kruysbergen

Windowcleaners

Zeven virusscanners vergeleken

Iedere Windows-gebruiker is inmiddels overtuigd van de noodzaak om aan virusbescherming te doen. Toch zijn antivirusprogramma's niet erg populair. Ze maken het systeem langzamer, onderbreken het surfen op internet en schreeuwen moord en brand bij onschuldige toepassingen.

Eén verkeerde klik en je Windows-computer is geïnfecteerd door een virus. Dat geldt niet alleen voor het besturingssysteem, maar ook voor heel veel toepassingen. Java en Flash zijn door geprepareerde online-applets te kraken en Adobe Reader is door schadelijke code met schijnberekeningen onderuit te halen. Zelfs fotoviewers kunnen door gemanipuleerde bestanden de deur openzetten voor malware die je

computer overneemt. Als Windows-gebruiker kun je dan ook niet zonder een virusscanner.

In deze test treden zeven commerciële antivirusprogramma's tegen elkaar in het strijdperk: Bitdefender AntiVirus Pro 2011, F-Secure Anti-Virus 2011, G Data AntiVirus 2011, Kaspersky Anti-Virus 2011, McAfee AntiVirus Plus 2011, Norton AntiVirus 2011 en Trend Micro Titanium AntiVirus Plus 2011. Deze moesten niet alleen hun kunsten op het gebied van bescherming bewijzen, maar ook laten zien hoe goed ze eenmaal aanwezige malware weer konden opruimen.

AVG Anti-Virus 2011 hebben we niet mee getest, omdat de definitieve versie pas na het begin van onze enkele weken durende test verscheen. Van Avira Antivir 10 en Panda 2011 zijn ook gratis versies beschikbaar, vandaar dat we deze nu niet hebben meegenomen.

Alle producenten verkopen ook complete security-pakketten met personal firewall, spamfilter en antiphishing. Die laten we hier buiten beschouwing. Het gebruik van deze extra's is op zijn minst discutabel, zie onder meer de test van gratis firewalls in deze c't op pagina 120. Het blijkt dat de firewall van Windows zelf prima voldoet. Outlook, Thunderbird en dergelijke hebben zelf al spamfilters aan boord en browsers als Firefox en Internet Explorer beschikken al langer over een ingebouwd phishingfilter. Vandaar dat we ons hier alleen op de virusscanners concentreren, al hebben een aantal virusscanners ook een eigen firewall. Overigens worden Windows Defender en Windows Firewall soms door het installatieprogramma van de antivirus uitgeschakeld zonder dat je daar om gevraagd hebt.

Een goede virusscanner probeert een malware-aanval te voorkomen door middel van meerdere mechanismen. Sommige daarvan werken na elkaar, andere tegelijkertijd. De eerste verdedigingslinie is de browserplug-in, die toegang tot bekende kwaadwillende websites blokkeert of in ieder geval een waarschuwing geeft dat je je in een gevaarlijk gebied bevindt.

De realtime-bewaking controleert het bestandsverkeer en toegang tot lokale bestanden. Daarmee moet verhinderd worden dat malware op je computer belandt. Sommige scanners controleren bestanden tijdens het downloaden al, anderen wachten tot zij volledig zijn binnengehaald of geopend worden.

De traditionele scanners komen op gezette tijden in actie om eerst de belangrijkste systeemonderdelen en daarna het hele systeem te controleren. Als de computer op de ingestelde tijd niet aan staat, haalt de virusscanner dat zo snel mogelijk weer in. Sommige scanners gaan pas echt aan de slag als de computer weinig tot niets te doen heeft (idle-scan). Dan heb je daar zelf het minste last van. Maar het kan ook irritant zijn dat je computer op volle toeren aan het werk is, terwijl je net nietsvermoedend even koffie hebt gehaald. Als je dan de muis even beweegt, keert de rust weer terug.

In principe beoordelen de bewaking en de scanner de bestanden op identieke criteria. Eerst kijken ze in een lokaal opgeslagen database van virusdefinities of een bestand een bitpatroon bevat dat daarin staat. Vervolgens wordt er een heuristiek gebruikt om te zoeken naar verdachte eigenschappen als bepaalde headerstructuren. Soms wordt een bestand dan zelfs in een interne sandbox uitgevoerd om te kijken of er iets onreglementairs gebeurt.

De laatste verdedigingslinie is de gedragsherkenning. Die let bij het uitvoeren van programma's op verdachte signalen. Ook bij de systeembewaking wordt gedragsherkenning gebruikt. Een Intrusion Detection System (IDS) beoordeelt of benaderingen van systeemfuncties niet op een aanvalspatroon lijken. Als een programma niet helemaal koosjere dingen lijkt te doen, kan de bewaking verschillend streng reageren. Sommige antivirusprogramma's geven alleen een waarschuwing, andere halen het proces zonder pardon uit het geheugen.

Performance-tuning

Om de systeembelasting te reduceren controleren veel realtime-bewakers geen ZIP- of andere archiefbestanden. De on-demand-scanner gaat in dit opzicht grondiger te werk, hij pakt ieder afzonderlijk bestand en kijkt in ieder archief.

Antivirusprogramma's proberen op deze en andere manieren om een balans te vinden tussen een hoog scanniveau en een zo laag mogelijke computerbelasting. Met uitzondering van Trend Micro Titanium Anti-Virus Plus slaan alle hier geteste scanners de checksums van al geanalyseerde bestanden op. Bij een volgende scan hoeven de als onverdacht geclassificeerde bestanden alleen nog vergeleken te worden met de signaturen die er sinds de laatste scan zijn bijgekomen in plaats van alle mogelijke malwarepatronen af te moeten lopen. Bij BitDefender, F-Secure, G Data en Norton liep een tweede systeemscan die meteen na de eerste werd gestart tot 95 procent sneller. Sommige scanners controleren eerder bekeken bestanden wel opnieuw na een update van de virusdefinities – om er zeker van te zijn dat er geen malware in het systeem zit die pas door een latere versie herkend kan worden.

Inmiddels onderhouden alle hier geteste programma's contact met hun makers om bestanden te analyseren (in-the-cloud-analyse). Een scanner kan bij een actieve internetverbinding dan ook malware vinden die nog niet in de lokale virusdatabase staat en ook niet een bepaald heuristiekpatroon volgt. McAfee bijvoorbeeld leunt sterk op deze methode. Norton AntiVirus beoordeelt de betrouwbaarheid van bestanden onder andere aan de hand van hun verbreiding, maar ook aan de hand van hun beoordeling door andere gebruikers (reputation-based services).

Het gebeurt steeds weer dat een virusscanner door een hyperactieve heuristiek of een verkeerde virusdefinitie zelfs essentiële systeembestanden in quarantaine zet. In het ergste geval legt dat meteen de hele computer plat – waarmee vernield wordt wat nu juist beschermd had moeten worden.

Door het uitbalanceren van de virusherkenning en de beoordeling op betrouwbaarheid, willen de makers dergelijke problemen verhinderen. Het lijkt immers hoogst onwaarschijnlijk dat een bestand plotseling een virus blijkt te zijn, terwijl het door duizenden computeraars gebruikt wordt en al sinds het installeren van het besturingssysteem op de harde schijf staat. Op basis van dergelijke feedback worden whitelists aangemaakt van processen waar je niet ongerust over hoeft te zijn. Dat moet verhinderen dat een scanner bij een defecte heuristiek of virusdatabase zulke processen per ongeluk deactiveert.

Bij een in-the-cloud-analyse hoort ook dat de virusscanner onbekende bestanden naar de producent stuurt. Deze kan daardoor snel op bedreigingen reageren. Alle producenten garanderen dat de toegezonden bestanden anoniem geanalyseerd worden en dat er geen persoonlijke gegevens geregistreerd worden. Als je dat niet vertrouwt, dan schakel je dit feedbacksysteem uit. Dat kan bij de meeste programma's meteen bij het installeren, alleen bij F-Secure en Trend Micro kun je die functie pas na het installeren bij de instellingen deactiveren.

De in-the-cloud-herkenning is ook weer geen wondermiddel. De eerste ontvangers van een nieuwe malwarevariant worden waarschijnlijk niet of slechts ten dele door hun virusscanner beschermd. Als alles goed is, ontdekt de virusscanner de malware later alsnog na een update van de virusdefinities en kan de schade die het kwaadwillende programma aangericht heeft weer ongedaan worden gemaakt. Bewaken en scannen is dan ook pas het halve werk. De antivirusprogramma's moeten de computers ook weer schoon kunnen maken door draaiende malwareprocessen te stoppen, belangrijke systeemcomponenten te reactiveren en alle bestandsdelen van de malware te verwijderen.

Testmethode

Alle scanners doorliepen een uitgebreid testtraject, waarbij de laboratoriumtests van antivirusspecialist AV-Test gebruikt werden. Alle tests werden op een identiek quadcore-systeem en een 32-bit versie van Windows 7 uitgevoerd. Eerst werd ieder antivirusprogramma op een verzameling van meer dan 300.000 malwarevarianten los-

gelaten, die AV-Test op zijn servers verzamelt. Het herkennen van scareware en soortgelijke scam- en oplichtingsprogramma's staat apart in de tabel.

De werking van de heuristiek werd getest door de scanners met twee weken oude virusdefinities op een systeem zonder interverbinding los te laten op bijna 24.000 stuks recente malware. Bovendien registreerde AV-Test gedurende een periode van twee weken hoe snel de antivirusproducenten nodig hadden om hun scanners met nieuwe dreigingen bij te werken (zero-day threats).

Achttien schadelijke programma's stelden de reinigingskracht van de virusscanners op de proef. Ze moesten de malware herkennen, deactiveren en alle sporen compleet verwijderen. De rootkit-scan werd met tien exemplaren gedaan. Dat zijn er niet zoveel, maar dat komt omdat deze methode om iemands computer over te nemen het onder Windows 7 en Vista veel moeilijker heeft dan onder Windows XP. Het herkennen van actieve en inactieve rootkits werd getest, evenals het verwijderen ervan.

De gedragsherkenning moest 22 malwarevarianten opsporen. Deze zijn langs de virusherkenning en de heuristiek gekomen en konden dus alleen nog opvallen door hun gedrag tijdens het uitvoeren. Ook hoorde hier een test van fout-positieven (false positives) bij. Hiervoor werden algemeen bekende, goedaardige programma's geïnstalleerd en uitgeprobeerd – de beoordeling houdt daarbij zowel rekening met fout-positieven van de bewaking als met gevallen waarbij de gedragsherkenning het uitvoeren van programma's tegenhield. AV-Test testte dit met meerdere datasets, waaronder Office- en Windows-bestanden en programma's van bekende downloadportals. Daarnaast kregen de scanners een aantal exotische bestanden voorgeschoteld, waaronder pc-demo's en game-trainers.

Bovendien werd gekeken hoeveel de virusscanner de systeemperformance beïnvloedde. Dat werd onder andere gedaan met een meting van de tijd die het systeem nodig had om op te starten en af te sluiten, evenals de vertraging bij het aanmaken van een reeks bestanden met vergelijkbare inhoud. Die metingen werden vergeleken met de performance van hetzelfde systeem zonder geïnstalleerde virusscanner en vervolgens omgerekend naar percentages.

Omgangsvormen

Deze test maakt duidelijk dat scanprestaties niet alleenzaligmakend zijn. Zelfs de beste engine kan er niet aan ontkomen dat de software zich continu met weinig hulpvaardige waarschuwingen naar de voorgrond dringt. Aan de andere kant kan een aangenaam te bedienen interface geen krachtige schoonmaakroutines vervangen.

Om de werkbaarheid van de scanners in de standaardinstellingen te testen, werden ze op twee productiecomputers geïnstalleerd. Op die manier was het beste te achterhalen hoe ze zich bij mailen, surfen, schrijven en bestandsoperaties gedragen.

Bovendien stonden er wat inactieve uitgepakte malwarebestanden in mappen, waar de scanners op verschillende tijden alarm voor sloegen. Soms zelfs pas op het moment dat we die gingen uitvoeren. We hadden ook een aantal fout-positieven op de computer staan, waaronder de genoemde pc-demo's. Hierbij ging het minder om het herkennen, maar vooral om hoe de antivirusprogramma's van zich zouden laten horen.

BitDefender AntiVirus Pro 2011

BitDefender is zowel voor beginners als gevorderden bedoeld. Daarom biedt het product drie interfaces van een verschillende complexiteit: de Basisweergave, Gemiddelde Weergave en Gevorderdenweergave. Bij zowel de statische malwareherkenning als de gedragsanalyse laat het Roemeense programma een zeer goede indruk achter, die echter weer gerelativeerd wordt door de gebruikersinterface.

Voor het installeren start BitDefender eerst een Quick Scan met virusdefinities van internet. Het is enigszins verrassend dat het installatieprogramma je laat kiezen om Windows Defender en Windows-firewall te deactiveren – het goede nieuws: je krijgt hier in ieder geval de keuze.

Na de installatie start BitDefender op de achtergrond een volledige scan – als je dat bij het installeren niet uitgezet hebt tenminste. Dat is vanuit veiligheidsoogpunt wel lovenswaardig, maar betekent ook dat de computer het een tijdje druk heeft.

In vergelijking met de vorige versie is er wat de interface betreft niet veel veranderd. De nieuw skin is donkerblauw, de vensters van de Basisweergave en van de Gemiddelde Weergave zijn groter, de Gevorderdenweergave is daarentegen weer iets kleiner geworden.

De Basisweergave biedt vier knoppen, waarbij er bij twee een configureerbaar menu openklapt waar je extra items aan toe kunt voegen. Het is onbegrijpelijk dat uitgerekend de onlinehulp alleen met administratorrechten te openen is.

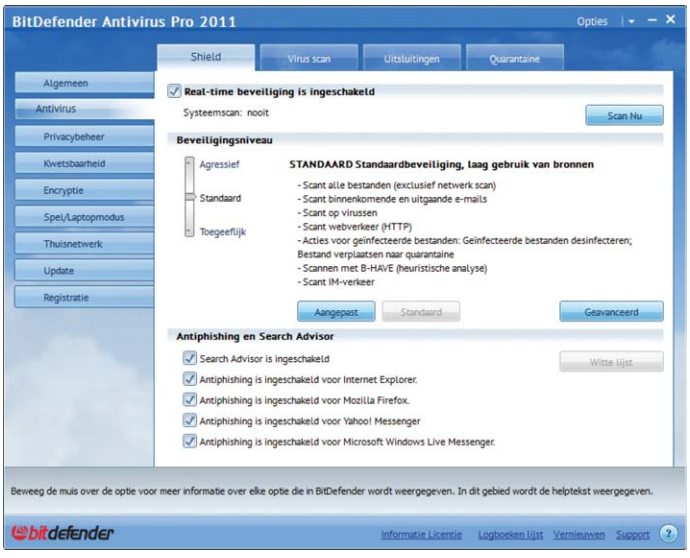
De Gemiddelde Weergave heeft een veld voor maximaal 13 functies. Hier zijn ook zelfgedefinieerde scantaken neer te zetten om die met een muisklik te kunnen uitvoeren. Meer dan vijf moet je er niet inzetten, omdat je anders heen en weer moet scrollen om de rest te zien te krijgen.

De Gevorderdenweergave is alleen voor echte mannen. In deze modus staat alles in één venster wat bij de andere modi over meerdere configuratiedialogen verspreid staat – dat zou handig kunnen zijn, ware het niet dat het zo onoverzichtelijk is. Negen tabbladen aan de linkerrand verdelen de functies in deelgebieden, die op hun beurt weer een aantal extra tabbladen bovenaan het scherm hebben. Ook al lijkt de structuur redelijk geslaagd, je ontkomt er niet aan om een rondgang door alle opties te maken.

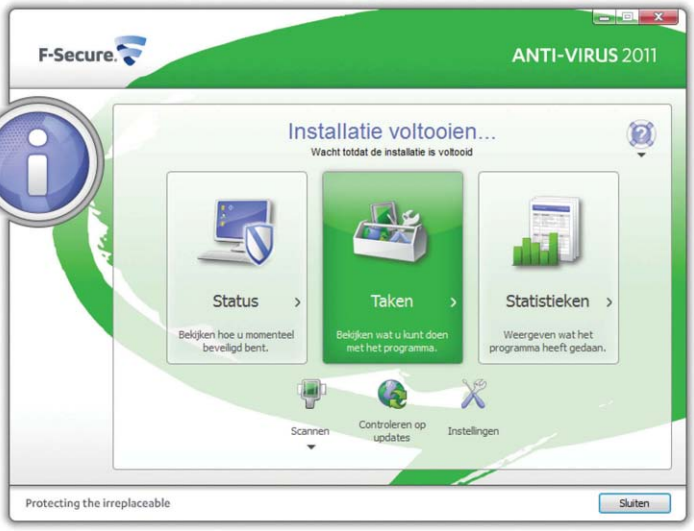
Als je bij de instellingen van de virusscanner bij het tabblad 'Shield' op de knop 'Geavanceerd' klikt, zie je op het tabblad 'IDS' van het venster dat dan verschijnt tot je grote verbazing dat het 'Inbraakdetectiesysteem' standaard gedeactiveerd is. Maar als je dat eenmaal geactiveerd hebt, kom je al snel achter de reden: er wordt aardig wat met valse meldingen gestrooid.

Tijdens de test ging de gedragsherkenning van het actieve virusbeheer zelfs op het laagste niveau 'Toegeeflijk' niet bepaald zachtzinnig om met alles wat hem niet aanstond. Als een MP3-tag-editor een browservenster wilde openen, werd dat door de virusscanner meteen verboden. Het installatieprogramma van een vectortekenprogramma en een duplicaatzoeker ondergingen hetzelfde lot – in deze gevallen leidden de heftige harddiskactiviteiten tot argwaan. In deze toestand is met de intrusion detection niet meer zinvol te werken. Dat is eigenlijk wel verrassend, omdat de gedragsherkenning het in de laboratoriumtests zelfs zonder IDS zeer goed deed.

De voortgang van de virusscanner wordt door BitDefender



Bij BitDefender Antivirus Pro 2011 staan in de Gevorderdenweergave alle configuratiemogelijkheden bij elkaar. De Basisweergave en de Gemiddelde Weergave zijn minder vol.



F-Secure Anti-Virus 2011 is makkelijk te bedienen en heeft duidelijk aan snelheid gewonnen. De gedragsherkenning laat zich echter wel erg vaak horen.

centraal in een groot venster getoond. De resultaten worden in een XML-bestand weggeschreven, dat in Internet Explorer geopend wordt. Om daar ook alle informatie te kunnen zien, moet je iedere keer op 'Geblokkeerde inhoud toestaan' klikken. Oudere scanberichten zijn in te kijken door te klikken op 'Logboeken lijst / Antivirus' en dan te dubbelklikken op de betreffende taak.

Vreemd genoeg verwijderde BitDefender sommige als malware geïdentificeerde bestanden meteen in plaats van ze in quarantaine te zetten. Dat het daarbij ook om echte malware ging, was alleen een schrale troost. Het was enigszins irritant dat BitDefender tijdens de updates in de testperiode bijna dagelijks om een herstart vroeg.

De Nederlandse versie heeft soms nog een verdwaalde Engelse term of een kromme zinsconstructie ("Nee, ik wil niet liever geen e-mailadres invoeren").

Onder de interface verschuilt zich een echt goede scanengine, die ook niet al te veel performance opslokt. BitDefender herkende bijna 98 procent van de malware en viel (bij uitgeschakelde IDS) niet op door valse alarmen (fout-positieven).

De desinfectierate bij malwarebesmetting en rootkits zag er minder goed uit. Bij één van de 18 wormen en drie van de 10 rootkits was BitDefender machteloos. De gedragsherkenning achterhaalde slechts één van 22 virussen. Het lukte BitDefender ook maar in acht gevallen om de gevonden virussen compleet te verwijderen.

F-Secure Anti-Virus 2011

De uit Finland afkomstige virusscanner van F-Secure is bijna de tegenpool van BitDefender: een eenvoudige interface met weinig dialoogvensters en overzichtelijke instellingen. F-Secure Anti-Virus heeft geen phishingbescherming voor de browser, dat zit alleen in het Internet Security-pakket van deze fabrikant.

De interface is sinds de vorige versie grotendeels hetzelfde gebleven. Het hoofdvenster biedt drie grote en drie kleinere knoppen, waarbij de 'Scannen'-knop een drop-downmenu is, dat toegang tot verschillende scanmogelijkheden biedt. In het statusvenster zijn de scanner, de gedragsherkenning en de regelmatige scans nu aan of uit te zetten – eerder meldde dit venster alleen de actuele status. De Taken-dialoog heeft knoppen voor alle essentiële programmafuncties en toegang tot de quarantaine. Via 'Statistieken' kom je bij taartdiagrammen met informatie over de systeemveiligheid.

Alle instellingsmogelijkheden passen in één dialoogvenster met negen onderdelen. 'Scannen volgens planning' staat standaard gedeactiveerd. F-Secure Anti-Virus gaat dus niet uit zichzelf de hele computer afstropen. Wel jammer dat de frequentie van het updaten van de virusdefinities (eens per twee uur) niet aan te passen is.

De gedragsherkenning 'DeepGuard' is duidelijk veranderd ten opzichte van de vorige versie. In de standaardmodus slaat de controle nog steeds bovenmatig vaak alarm. Een FTP-uploader en een tool voor bestandssynchronisatie werden als schadelijk beoordeeld en afgesloten. Je kunt wel redelijk makkelijk uitzonderingen definiëren. Bij sommige programma's kan dat zelfs via een directe link in het dialoogvenster, waarmee het configuratievenster voor uitgesloten items geopend wordt.

F-Secure categoriseert programma's als malware of riskware. In het laatste geval heb je de mogelijkheid het bestand uit te sluiten van scannen. Maar zelfs als je dat uitdrukkelijk wilt, verschijnt de melding dat de riskware geblokkeerd is – dat is er bij de kwaliteitscontrole waarschijnlijk doorheen geglipt.

Volgens de producent houdt de gedragsherkenning bij het beoordelen ook rekening met de ervaringen van andere gebruikers. Tijdens de test was daar echter weinig van te merken, het oordeel was altijd 'onbekend'. De lange denkpauzes bij het verwijderen van malware in de vorige versie behoren nu tot het verleden. Als F-Secure meerdere virussen vindt, krijg je voor ieder virus na elkaar hetzelfde venster met de melding dat het betreffende virus verwijderd is.

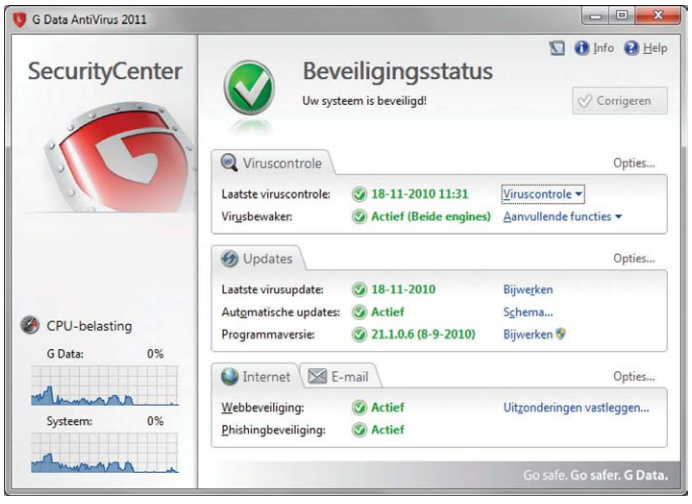
De scanengine komt van BitDefender, wat ook door de vergelijkbare resultaten wordt bevestigd. F-Secure lijkt echter een eigen algoritme toegevoegd te hebben. Anti-Virus herkende bijvoorbeeld een actieve rootkit die door BitDefender niet gevonden werd. F-Secure kon ook twee keer zoveel via de gedragsherkenning opgespoorde virussen weer verwijderen. Bij het verwijderen van andere malware deed F-Secure het echter wat minder en bij de gedragsherkenning glipte een programma door de controle heen, dat door BitDefender wel herkend werd.

G Data AntiVirus 2011

G Data wil na het installeren je computer meteen herstarten en begint dan meteen met een 'Snelle viruscontrole'. Daarna wil G Data AntiVirus pas bijgewerkt worden.

Na het updaten verrast het hoofdvenster met de melding dat het systeem al een lange tijd niet meer gecontroleerd is – dat verandert pas na een complete systeemscan. Daar had G Data op een testcomputer wel eerst 15 uur voor nodig, later 20 uur en 31 uur – om daarna na 2 uur al klaar te zijn.

Bij de vorige versie had de programma-interface bijna overal administratorrechten voor nodig. Bijna bij iedere klik kwam het Gebruikersaccountbeheer (User Account Control, kortweg UAC) naar boven. In de 2011-versie is dat anders. Er staan wel UAC-waarschuwingsbordjes, maar als je die aanklikt wordt het Gebruikersaccountbeheer niet actief. Zelfs voor het afsluiten van de scanner heb je geen administratorrechten nodig – alleen bij scans wordt het venster nog donker. Als je



In G Data AntiVirus 2011 zitten twee scanengines. Fout-positieven zijn door een whitelist te voorkomen.

dan toegang weigert, slaat G Data AntiVirus de systeemdelen over.

Het hoofdscherm ziet er wat opgeruimder uit dan voorheen, het meeste is echter hetzelfde gebleven. Aan de linkerkant laten grafieken de algemene processorbelasting en het concrete aandeel van G Data zien. De configuratiemogelijkheden zitten verspreid over meerdere dialogen met tabbladen en subdialogen in plaats van gebundeld op een centrale plek.

Er zijn meerdere mogelijkheden om met geïnfecteerde bestanden om te gaan – desinfecteren, in quarantaine zetten, verplaatsen of verwijderen. De scanner heeft een ietwat curieuze voorstelling van het begrip desinfecteren: de vermeende malware wordt vervangen door een bestand met dezelfde naam, maar dan met een grootte van 0 bytes. Daarom moet je bij de opties van de virusscan instellen dat hij geïnfecteerde bestanden standaard in quarantaine zet, en niet probeert ze te desinfecteren.

Als G Data actieve malware vindt, wil het eerst herstarten voordat met opruimen wordt begonnen. Dat is een verstandig idee. Maar onder bepaalde omstandigheden wil de scanner bij het vinden van een inactief virus ook herstarten, en dat is dan totaal overbodig.

G Data gebruikt net als F-Secure de engine van BitDefender, maar heeft daar de scantechnologie van Alwil (Avast) aan toegevoegd. Twee scanners dus, wat ook tot een dubbele bescherming zou moeten leiden – G Data is inderdaad dan ook het enige geteste programma dat bij de herkenningsscore boven de 99 procent uitkomt. Bij de rootkitanalyse waren G Data AntiVirus en Norton de enige scanners die alle programma's herkenden en voor honderd procent konden verwijderen. Bij de gedragsherkenning ziet het er echter een stuk minder roosskleurig uit, daar staat G Data op de op één na laatste plaats.

Een belangrijke zorg bij twee scanners is dat het aantal valse alarmen ook kan verdubbelen. Bij vorige versies van G Data bleek dat alle valse alarmen van BitDefender 1-op-1 werden overgenomen. Versie 2011 heeft een eigen whitelist waardoor dit probleem nu verrassend goed onder controle is. Afgezien van twee demo's en een game-trainer viel de scanner verder niets te verwijten.

De twee kloppende harten van G Data AntiVirus hebben toch wel een nadeel: als de scanner volledig los gaat, wordt de computer duidelijk afgeremd. Een systeemscan moet je dan ook alleen op een tijdstip doen waarop je niet achter de computer zit. Al met al maakt de 2011-versie een duidelijk snellere indruk dan de vorige. Alleen bij een van de synthetische performancetests was er een uitschieter. Het aanmaken van 10.000 vergelijkbare bestanden duurde namelijk honderd keer zo lang als zonder virusscanner. Maar omdat je dat bij normaal computergebruik eigenlijk nooit doet, hebben we deze uitschieter niet in de performancebeoordeling meegenomen.

Kaspersky Anti-Virus 2011

Kaspersky heeft bij ervaren gebruikers een goede naam: een stabiele engine, weinig foutpositieven en een groot aantal instelmogelijkheden om het scannen aan je wensen aan te passen. De 2011-versie wil met een vereenvoudigde interface ook technisch minder onderlegde gebruikers aanspreken.

De eerste Revision van Kaspersky Anti-Virus 2011 had dusdanig veel fouten dat er al snel een Critical Fix 1 verscheen. Een van de testcomputers bevroor tijdens het updaten van de virusdefinities telkens weer. Bij het opnieuw starten meldde Kaspersky dan dat bepaalde interne databases beschadigd waren. Te oordelen aan de reacties in de gebruikersforums is dat echter geen uitzondering.

Bij het testen viel Kaspersky meerdere malen op door buitengewone performance-uitschieters. Het openen van een map met 200 bestanden duurde bijvoorbeeld onverklaarbaar lang. Voor het 20.000 keer kopiëren van een bestand had de scanner twee keer zo lang nodig als de concurrentie. Begin oktober verscheen een tweede Critical Fix, die na een paar dagen weer naar een bètastadium werd teruggehaald – deze test is dan ook met de Critical Fix 1 (Build 11.0.1.400.a) gedaan.

Het hoofdscherm is overzichtelijk ingedeeld in vijf tabbladen. Via 'Upgrade' kom je alleen bij een uitnodiging om de Internet Security-suite 30 dagen te proberen. Op de andere vier tabbladen staan de functies overzichtelijk gegroepeerd. Het startschem heeft drie uitklapbare delen, waarin je alle modules apart kunt uitzetten. Het item 'Instellingen' in het menu van iedere module leidt tot een uitgebreide maar nog net overzichtelijke instellingsdialoog voor de betreffende module.

Kaspersky Anti-Virus is heel gedetailleerd te configureren. Net als bij BitDefender zijn veel instellingen via schuifregelaars aan te passen, waarbij een klik op de knop 'Instellingen' nog meer configuratiemogelijkheden geeft. Als je per ongeluk iets verkeerd doet, kun je de begintoestand voor de afzonderlijke modules weer herstellen.

De interface van Kaspersky Anti-Virus 2011 ziet er goed uit, de scanperformance blijft daar wat bij achter.

Onder 'Tools' biedt het programma de mogelijkheid om een op Linux gebaseerd noodmedium te maken. Kaspersky download dan eerst een ISO-image van internet en zet daar de laatste virusdefinities op. Daarbij worden in principe zowel optische als usb-media ondersteund, maar in de test werkten alleen de gebrande cd's.

Kaspersky komt de hele tijd met kleine statusmeldingen rechtsonder op het beeldscherm van de gedragsherkenning. Die zijn sneller weer verdwenen dan je ze kunt lezen. Deze venstertjes hebben verschillende kleuren en bevatten alleen cryptische afkortingen in plaats van begrijpelijke beschrijvingen. Je kunt vanuit het statusvenster in ieder geval uitzonderingen definiëren om bepaalde meldingen gericht uit te schakelen.

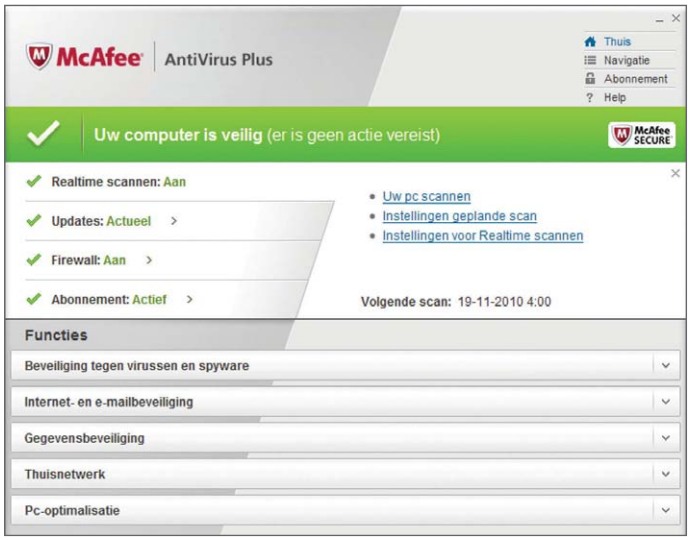
Bij de laboratoriumtest deed Kaspersky het goed, maar niet geweldig. Bij het scannen van de malware kwam Kaspersky op de laatste plek terecht, maar herkende altijd nog 96 procent. Bij het desinfecteren scoorde de scanner gelijk met Norton, maar achter BitDefender en F-Secure. Kaspersky herkende ook alle rootkits en kon er slechts één niet compleet verwijderen. De gedragsherkenning herkent bedreigingen erg goed, maar het programma kon maar de helft van de op die manier geïdentificeerde virussen verwijderen.

McAfee AntiVirus Plus 2011

De Plus in de naam komt omdat McAfee buiten de feitelijke scanner ook een personal firewall, een systeemschoonmaaktool en de browserplug-in SiteAdvisor meelevert. Als je voor een aangepaste installatie kiest, dan kun je alle niet benodigde onderdelen weglaten en later eventueel nog toevoegen.

Bij het installeren wil McAfee meteen de laatste software downloaden (zo'n 110 MB), maar je kunt er ook voor kiezen dat over te slaan en de versie van de cd te installeren.

De oerlelijke interface van de voorgaande versie is verdwenen, het nieuwe hoofdvenster heet 'Thuis' en ziet er overzichtelijk en vriendelijk uit. Maar schijn bedriegt, veel verschillend genoemde menu-items leiden tot



Bij McAfee AntiVirus Plus 2011 is de eerste positieve indruk misleidend: de scanner biedt je niet eens de mogelijkheid om uitzonderingen toe te voegen.

dezelfde dialogen. En als je naar een optie zoekt om bestanden of mappen uit te sluiten van een scan, blijf je vroeg of laat in een kringetje ronddraaien.

Daar komt bij dat de hoogte van het hoofdvenster vast staat op 650 pixels. Een aantal dialogen past daar echter niet in, zodat je bijvoorbeeld bij de scaninstellingen heen-en-weer blijft scrollen. Een puur uit tekst bestaand 'Navigatiecentrum' leidt overwegend tot dezelfde dialogen, maar ook tot de virusquarantaine, die op het hoofdvenster weer ontbreekt.

Als de scanner een potentieel ongewenst programma meldt, kun je toestaan dat dat uitgevoerd wordt. Als McAfee AntiVirus Plus echter denkt een trojan te herkennen, dan is er geen genade, als je het bestand uit de quarantaine haalt, wordt het daar meteen weer in teruggestopt. McAfee was het enige programma dat geen mogelijkheid had om een eenmaal als trojan geclassificeerd bestand uit te sluiten van de bewaking.

McAfee deed het bij de laboratoriumtests helemaal niet slecht. De scanner herkende bijna 99 procent van de virussen en rootkits. Bij de gedragsherkenning haalde AntiVirus Plus een percentage van 82 procent. De zero-day-herkenning was de beste in deze test. Maar wat deze kale cijfers niet verraden is, dat de goede prestaties gekocht zijn.

McAfee heeft de herkenning namelijk uitbesteed en een echte gedragsherkenning is er dan ook niet. AntiVirus Plus stuurt de verdachte bestanden gewoon naar de eigen online-scanner, die de analyse dan op zich neemt. Een fataal gevolg van deze outsourcing is dat McAfee drie keer zoveel fout-positieven geeft dan de slechtste concurrent – dat is bij een scanner zonder een uitzonderingslijst eigenlijk ontoelaatbaar.

Ook bij het desinfecteren zijn de resultaten niet overweldigend. Van de 18 actieve virussen wist McAfee er maar 3 volledig te verwijderen. Bij het verwijderen van rootkits was de software met slechts drie succesvolle opschoningen met afstand de slechtste.

De Site Advisor is een (gratis) plug-in voor Firefox en Internet Explorer en markeert websites groen, geel of rood. Meer informatie krijg je dan in een tekstballon of in een uitvoerig Sitereport. Als je meer wilt dan alleen waarschuwingen, kun je bij de configuratieopties 'Securezoeken' inschakelen, maar dat is eigenlijk niet meer dan een uitgebreide Yahoo-toolbar.

Norton AntiVirus 2011

Het installeren van Norton AntiVirus gaat veruit het snelst. Het programma last daarna een kunstmatige pauze van een half uur in, voordat de eerste update van de virusdefinities wordt uitgevoerd. Maar die kun je ook handmatig starten. Als je een internetverbinding hebt, controleert de scanner iedere vijf minuten op de server of er nog wat nieuws is – de veruit hoogste updatefrequentie in deze test.

Het overzichtelijke hoofdvenster heeft acht knoppen om verschillende componenten te deactiveren. In het onderste deel staat een wereldkaart met in het geel de 'cybermisdaad'. Een klik op de kaart opent een ticker met de steden met de meeste bedreigingen – wat de meerwaarde daar ook van mag zijn. Het nut van de knop rechtsonder is nog discutabeler, die komt met reclame voor Nortons online opslagruimte.

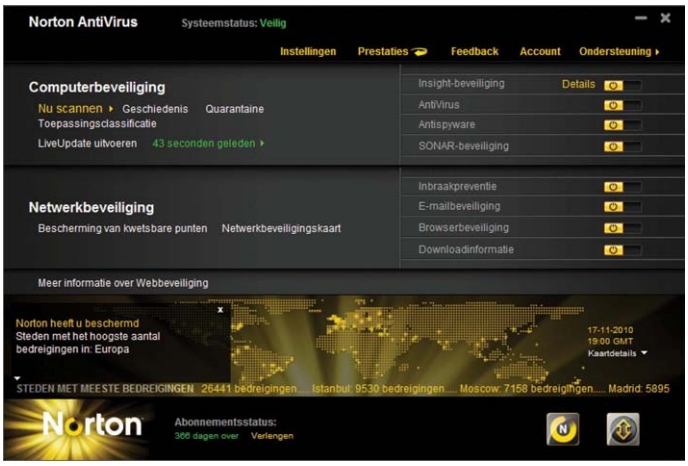
Als je op 'Prestaties' klikt, draait het hoofdvenster om zijn verticale as en laat dan diverse soorten systeeminformatie zien: de processorbelasting, een tijdlijn met informatie over scans, geïnstalleerde software en downloads. En dit tot op een ongewoon diep niveau. De boodschap zal ongetwijfeld zijn dat Norton overal een beschermende hand boven houdt. Sceptici denken eerder aan 'Big Norton'.

Symantec blijft bij een gebruikersbasis om de betrouwbaarheid van bestanden te beoordelen. Na het installeren begint Norton AntiVirus de lopende processen te analyseren op verspreiding en resourcegebruik om die buiten beschouwing te laten bij virusscans (File Insight). Maar af en toe loopt het gebruik van de community ook op niets uit. Tijdens de test kwam het vaker voor dat Norton bij het installeren van een pas verschenen software-update het bestand als niet betrouwbaar aanmerkte en een waarschuwing gaf.

Twee versies geleden was het dialoogvenster voor de instellingen nog een toonbeeld van overzichtelijkheid. Inmiddels zitten er in de hoofdcategorie al 31 knoppen en configuratiedialogen, dat is dus scrollen geblazen. Bovendien lijkt de indeling ietwat willekeurig. De frequente virusdefinitie-updates zijn onder 'Computerinstellingen' te deactiveren, het downloaden van nieuwe software-updates zit dan weer onder 'Diverse instellingen'. Je kunt nu wel de uitzonderingen voor de scanner en de realtime bewaking apart instellen. Dat lijkt in eerste instantie flexibeler te werken, maar in de praktijk leidt het vaak tot dubbel werk.

Het rescue-medium 'Bootable Recovery Tool' is gebaseerd op Windows PE. Een wizard maakt naar keus een bootable usb-stick of een cd/dvd met de laatste virusdefinities. Als je met de Recovery Tool een andere computer wilt scannen, wordt de productcode van 25 tekens gevraagd.

Bij het herkennen van actieve malware deed Norton het niet slecht. Bij de gedragherkenning glipten 7 van de 22 virussen er doorheen – dat was in de vorige versie beter en kan wellicht een uitzonderingsgeval zijn. De rootkits werden door Norton AntiVirus 2011 niet alleen allemaal herkend, maar ook compleet verwijderd. Van de actieve malware kon echter niet meer dan 61 procent volledig verwijderd worden. In twee gevallen bleef het virus zelfs op de computer staan. Bij de gedragsherkenningstest kon slechts de helft van de malware verwijderd wor-



Norton AntiVirus 2011 saboteert de in principe solide indruk door spektakelopsmuk als een knipperende wereldkaart met 'cybermisdaad'.

den, in vier gevallen bleef die ondanks de opruimactie op de computer achter.

Trend Micro Titanium AntiVirus Plus

Titanium AntiVirus Plus is veruit de vriendelijkste scanner in deze test. Een virusmelding eindigt bijvoorbeeld met de mededeling dat je verder niets hoeft te doen en de melding kunt sluiten.

Bij het installeren moet je per se een naam en een e-mailadres opgeven. Bij de eerste start verkondigt een hemelsblauw dialoogvenster trots: 'U hoeft nooit meer op een knop Bijwerken te klikken' – de software moet zichzelf automatisch updaten. De laboratoriumtest bracht echter aan het daglicht dat Titanium AntiVirus maar één keer per dag nieuwe virusdefinities ophaalt – wat veel te weinig is.

Het webfilter gaat in Chrome, Internet Explorer en Firefox in principe op dezelfde manier te werk. Bij een klik op een verdachte link verschijnt er in plaats van de verwachte website een waarschuwing met de keuze het venster weer te sluiten of op eigen risico verder te gaan. Als je de Firefox-extensie NoScript geïnstalleerd hebt, krijg je alleen de link van de geblokkeerde website te zien. Om dan verder te kunnen, moet je NoScript deactiveren – en dat uitgerekend voor een website die door het filter geblokkeerd is. Dat krijg je ervan als beveiligingsconcepten elkaar in de wielen rijden.

Het licht doorschijnende instellingenvenster is goed gestructureerd en verdeeld in vier delen. Een voor de virus- en spywarebesturing, een voor de internet- en e-mailbesturing, een voor de uitzonderingslijsten en dan nog een voor 'Overige instellingen'. Trend Micro laat je de keuze of de scanner gevaarlijke bestanden automatisch mag verwijderen en of er überhaupt waarschuwingen gegeven moeten worden. Met een drietrapsregelaar kun je instellen hoe ijverig het webfilter je tegen risicovolle websites moet beschermen.

Het beveiligingsoverzicht laat een bontgekleurd taartdiagram zien met de gevonden bedreigingstypen en een tijdlijn van de gevonden malware van de afgelopen maand.

Een betrouwbaar ogende interface garandeert echter nog geen goede prestaties bij het scannen en opschonen. Titanium AntiVirus kon bij de laboratoriumtest maar 3 van de 18 infecties helemaal verwijderen. Bovendien werden 2 van de 10 rootkits in inactieve toestand over het hoofd gezien. En bij de rootkitdesinfectie bleven in drie gevallen restanten achter.

De gedragsherkenning was ronduit de slechtste in de test, er werden maar 4 van de 22 virussen gevonden en daar kon maar de helft van verwijderd worden. Bij de algemene laboratoriumtest vielen weliswaar geen fout-positieven op, maar bij de testset met pc-demo's en game-trainers kwalificeerde Titanium AntiVirus zes van deze onschuldige programma's als malware.

Titanium remt de browser merkbaar af bij het browsen. En de mailclients Thunderbird en The Bat waren amper nog te gebruiken. Iedere wisseling van IMAP-map leidde tot een secondelange denkpauze. Bijlagen werden tergend langzaam aan te versturen mails toegevoegd. Dergelijke ernstige performanceverliezen waren bij geen enkele ander programma in deze test te zien.

Trend Micro Titanium AntiVirus Plus 2011 is het vriendelijkste programma in deze test, maar stelt wel teleur met slechte herkenningsresultaten.

Conclusie

Laten we op voorhand zeggen dat je je aan geen van de hier besproken programma's een buil kunt vallen. De scanresultaten op basis van virusdefinities en heursitieken liggen dicht bij elkaar. Bij de virusdefinities is 98 procent het minimum, de heuristiekscores variëren tussen 41 (McAfee, Trend Micro) en 66 procent (G Data). Bij de gedragsherkenning worden de verschillen echter significanter. G Data en Trend Micro vormen daar de achterhoede, maar ook Symantecs score ligt onder de 70 procent.

De grootste verschillen worden duidelijk als het erom gaat om een met malware besmette computer weer gezond te krijgen. Bij het standaarddesinfecteren moet je al blij zijn met de 83 procent die BitDefender biedt. McAfee en TrendMicro komen niet eens aan de 17 procent. Bij het verwijderen van rootkits overtuigen alleen G Data en Norton. BitDefender en TrendMicro kwamen daarbij niet verder dan zeven van de tien, McAfee kwam niet verder dan drie.

Als de laatste verdedigingslinie het af laat weten, ben je overgeleverd aan de malware. En net uitgerekend bij de gedragsherkenning waren de resultaten bijzonder slecht – geen enkele scanner kon alle gevaren afvangen. Als je dus de bewaking 'even' uitzet om een snel een programmaatje op de rand van de legaliteit uit te testen, loop je dus een enorm risico.

BitDefender kon 20 van de 22 virussen in ieder geval ten dele tegenhouden, maar wist er maar acht compleet te verwijderen. Bij Trend Micro glipten 18 aanvallers door de mazen heen. En maar alleen in twee gevallen wist de scanner het systeem weer helemaal schoon te krijgen.

Bij de laboratoriumtest waren relatief weinig fout-positieven te zien – met uitzondering van McAfee dan. De meeste fout-positieven kwamen op het conto van de testset met 17 pc-demo's, game-trainers en andere exotische software. Hier was één fout-positief het minimum (Kaspersky). Trend Micro zette maar liefst zes van deze (onschuldige) programma's meteen in quarantaine.

Als je vaker exotische, maar wel betrouwbare software ge-

Antivirus voor Windows

Programmanaam	
Producent	
Website	
Programmaversie	
Programmataal	
Ondersteunde Windows-versies (volgens producent)	
Updates per week / gemiddelde grootte	
Gem. reactietijd bij nieuw virus	
Kleinst mogelijke bijwerkinterval	
Functies	
Webfilter (alleen HTTP)	
Kies actie bij virus	
E-mail-flter	
Gedragsherkenning	
Installatie deactiveert Windows Defender	
Rescuemedium: meegeleverd / te maken / bij te werken	
Herkenning	
Definities: malwareverzameling van 328.057 virussen	
Definities: oplichterij / potentieel ongewenste programma's	
Heuristiek bij 2 weken oude definities	
Herkenning nieuwe malware de laatste 2 weken	
Desinfectie: herkend / gedeactiveerd / verwijderd (van 18)	
Actieve rootkits inactief / actief / verwijderd (van 10)	
Fout-positieven (van 165.997 schone bestanden)	
Performance	
Scantijd 4,5 GB: on-demand / on-access	
Snelheid testsuite met bewaking[2]	
Geheugenverbruik Working Set / virtueel / virtueel max.	
Gedragsherkenning	
Schadelijke software herkend / geblokkeerd (van 22)	
Veilige progamma's gemeld / geblokkeerd (van 16)	
On-demand-scanner: scandiepte	
Archieven: enkelvoudig / genest / zelfextr. (max. 11 / 6 / 6)	
Scan ingebedde objecten: OLE / Web-OLE / met wachtwoord (30 / 21 / 10)	
Beoordeling functies	
Definitieherkenning schadelijke software / scareware	
Herkenning heuristiek / rootkits / gedragsgebaseerd[3]	
Desinfectie definitiegebaseerd / rootkits / gedragsgebaseerd	
Definitie-updates en reactietijden	
Beoordeling gebruik	
Bedienbaarheid / gebruiksvriendelijkheid	
Onopvallendheid	
Subjectieve snelheid	
Prijs voor 1 jaar: nieuw (1 pc - 3 pc's) / upgrade (1 pc - 3 pc's)	

[1] alleen bij 'riskware', anders automatische actie
⊕⊕ zeer goed ⊕ goed ○ voldoende

BitDefender AntiVirus 2011	F-Secure Anti-Virus 2011	G Data AntiVirus 2011	Kaspersky Anti-Virus 2011	McAfee AntiVirus Plus 2011	Norton AntiVirus 2011	Trend Micro Titanium AntiVirus Plus 2011
BitDefender	F-Secure	G Data	Kaspersky Lab	McAfee	Symantec	Trend Micro
www.bitdefender.nl	www.f-secure.nl	www.gdata.nl	www.kaspersky.com/nl	www.mcafee.nl	www.symantec.nl	trendmicro.nl
14.0.23.312	10.50 build 197	21.1.0.5	11.0.1.400 (a)	10.5.195	18.1.0.37	3.0.1303
Nederlands	Nederlands	Nederlands	Nederlands	Nederlands	Nederlands	Nederlands
XP / Vista / 7 (ieder 32/64-bit)	XP / Vista / 7 (ieder 32/64-bit)	XP / Vista / 7 (ieder 32/64-bit)	XP / Vista / 7 (ieder 32/64-bit)	XP (alleen 32-bit) / Vista / 7 (ieder 32/64-bit)	XP (alleen 32-bit) / Vista / 7 (ieder 32/64-bit)	XP / Vista / 7 (ieder 32/64-bit)
112 / 980 kB	62 / 680 kB	117 / 780 kB	55 / 690 kB	7 / 120 kB	1646 / 355 kB	8 / 760 kB
4 tot 6 uur	2 tot 4 uur	2 tot 4 uur	4 tot 6 uur	4 tot 6 uur	2 tot 4 uur	4 tot 6 uur
1 uur	–	1 uur	5 minuten	–	–	–
✓	–	✓	✓	✓	✓	✓
✓	✓[1]	✓	–	✓[1]	✓[1]	–
✓	✓	✓	✓	–	✓	✓
✓	✓	✓	✓	✓	✓	✓
✓	–	–	–	–	✓	✓
✓ / – /✓	✓ /✓ /✓	✓ / – / –	– /✓ /✓	– / – / –	✓ /✓ /✓	– / – / –
97,8 %	97,9 %	99,5 %	96,4 %	98,9 %	98,9 %	98,7 %
99,2 % / 94,3 %	99,7 % / 94,3 %	99,9 % / 99,5 %	99,3 % / 88,7 %	99,3 % / 98 %	99,8 % / 95,2 %	99 % / 91,5 %
57,6 %	58,2 %	66,4 %	54,2 %	41,1 %	51,2 %	41,2 %
41,5 %	42,1 %	45,5 %	44,7 %	54,9 %	47,5 %	39,2 %
18 / 17 / 15	18 / 15 / 14	18 / 14 / 12	18 / 18 / 11	18 / 15 / 3	18 / 16 / 11	18 / 18 / 3
10 / 9 / 7	10 / 10 / 8	10 / 10 / 10	10 / 10 / 9	10 / 7 / 3	10 / 10 / 10	8 / 10 / 7
6	2	3	3	19	5	7
142 / 267	117 / 420	119 / 341	78 / 313	196 / 440	113 / 248	195 / 260
65,5 %	76,7 %	67,3 %	67,6 %	80,0 %	68,1 %	69,7 %
43 / 96 / 97 (MB)	66 / 120 / 120 (MB)	44 / 256 / 322 (MB)	52 / 75 / 97 (MB)	55 / 193 / 227 (MB)	26 / 23 / 52 (MB)	5 / 15 / 15 (MB)
21 / 20	21 / 18	11 / 7	20 / 16	18 / 17	15 / 11	4 / 2
1 / 0	1 / 0	0 / 0	1 / 0	0 / 0	0 / 0	0 / 0
11 / 6 / 6	11 / 6 / 6	11 / 6 / 6	11 / 6 / 6	11 / 6 / 6	11 / 6 / 6	11 / 6 / 6
30 / 21 / 10	30 / 21 / 10	30 / 21 / 10	30 / 21 / 10	30 / 21 / 10	30 / 21 / 9	30 / 21 / 10
⊕⊕ / ⊕	⊕⊕ / ⊕	⊕⊕ / ⊕⊕	⊕⊕ / ⊕	⊕⊕ / ⊕⊕	⊕⊕ / ⊕⊕	⊕⊕ / ⊕
○ / ⊕⊕ / ⊕	○ / ⊕⊕ / ○	⊕ / ⊕⊕ / ⊖	○ / ⊕⊕ / ○	⊖ / ⊕ / ⊖⊖	○ / ⊕⊕ / ○	⊖ / ⊕⊕ / ⊖⊖
⊕ / ⊕ / ○	⊕ / ⊕ / ⊕	⊕ / ⊕⊕ / ⊖	⊕ / ⊕⊕ / ○	⊖ / ○ / ⊕	⊕ / ⊕⊕ / ○	⊖ / ⊕ / ⊖⊖
○	⊕	⊕	○	○	⊕	○
⊖ / ○	⊕ / ⊕⊕	⊕ / ⊕	⊕ / ⊕	⊖ / ⊖	⊕ / ⊕	⊕ / ⊕⊕
⊖	⊖	⊖	○	○	○	○
⊕	⊕	○	⊖	○	⊕	⊖
€ 30 - € 50 / € 20 - € 40	€ 40 / € 35	€ 30 - € 40 / € 25 - € 33	€ 30 - € 40 / € 22 - € 30	€ 55 / € 55	€ 50 / € 40	€ 30 - € 40 / n.v.t.

[2] ten opzichte van 100 % zonder virusscanner; hoger = beter [3] zonder statische herkenning
⊖ slecht ⊖⊖ zeer slecht ✓ aanwezig – niet aanwezig n.v.t. niet van toepassing

bruikt, heb je aan BitDefender, F-Secure en Kaspersky duidelijk meer dan aan de producten van Symantec en Trend Micro. In dergelijke gevallen moet je McAfee in ieder geval niet gebruiken, omdat de foutief als malware geïdentificeerde programma's niet uit te sluiten zijn van toekomstige scans. Dat is niet acceptabel.

Een gebruiker wil meestal alleen dat een scanner zijn systeem zo goed mogelijk beschermt en daarbij voor zo min mogelijk hinder zorgt. BitDefender, Kaspersky en Norton houden daar enigszins rekening mee door over te gaan in een gamemodus als een programma fullscreen start. De scanners pauzeren dan hun virusdefinitie-updates, verschuiven eventuele virusmeldingen naar een later tijdstip en stellen geplande scans uit. Maar je moet je er wel van bewust zijn dat een betrouwbare realtime bescherming in principe altijd ten koste van wat performance gaat.

Bij de testsuite van AV-Test bleek McAfee wonderbaarlijk genoeg het beste, wat primair door de snelle online analyse komt en meteen ook het bovengemiddelde aantal fout-positieven verklaart. F-Secure komt op de tweede plaats. De andere porgramma's verschillen slechts marginaal van elkaar, maar hebben wel allemaal hun specifieke zwakke punten. Bij BitDefender en Trend Micro kost het controleren van gedownloade bestanden bijvoorbeeld veel tijd.

G Data start lekker snel, maar verbruikt ook het meeste werkgeheugen. De twee engines moeten hun virusdefinitiedatabases natuurlijk ergens kwijt. De verrassende performancedalingen bij Kaspersky duiden erop dat er hier nog wat te sleutelen valt. Het is te hopen dat de volgende Critical Fix snel komt. Norton AntiVirus remde het starten en het afsluiten van het systeem echter het meeste af.

Hoe relevant al deze resultaten in de praktijk zijn, hangt van het computergebruik af. Normaal valt een vertraging door de virusscanner alleen op bij grote kopieeracties, verder zijn de door de virusbescherming veroorzaakte vertragingen op een desktop-pc bij de meeste producten in deze test nauwelijks te merken. Dat is bij minder krachtige computers als netbooks wel anders. Daar trekt ook de minst belastende virusbescherming duidelijk aan de handrem. (nkr) c't