

Testmethode

Netwerkantimalwareproducten testen we in twee fasen: een antivirustest en een antimalwaretest. Bij virussen komt besmetting het meest voor doordat je een bestand binnenkrijgt via e-mail of een opslagmedium. Virusdetectie is dus een heel belangrijke eerste stap want die voorkomt dat je besmet raakt. Uiteraard moet er ook een achtergrondcontrole zijn die een eventueel tot dusver onbekend virus dat toch gestart is op je systeem, blokkeert. Een malwarebesmetting treedt heel vaak op een meer argeloze manier op: terwijl je surft, of eventueel ingebed in software die je installeert. Daarom lijkt ons de residente parasietblokkering de belangrijkste factor in de tweede fase van de test. Voor de antivirustest doen we daarom een detectie- en schoonmaakttest, en voor de antimalwaretest kijken we of de software in staat is een besmetting met honderden malware-objecten te voorkomen of, als dat toch lukt, het systeem met succes weer te zuiveren.

Naast deze prestatietesten hebben we ook punten gegeven op de functionaliteit en netwerkbeheerfaciliteiten van de diverse producten.

Antivirustest

Zoals je uit onze vorige testen wel weet, hebben we zelf een collectie van in deze contreien al voorgekomen virussen samengesteld. Onze collectie is eerder bescheiden, maar er zit wel van alles in. We hebben programmavirussen, macro- en scriptvirussen en speciale virussen die zich in allerlei andere bestanden proberen te verstoppen. Met virussen bedoelen we uiteraard in één adem ook trojans en wormen, kortom alles waarvan je verwacht dat een goed antiviruspakket je ertegen beschermt. Onze collectie omvat bijna achttienduizend stuks.

Helaas bleek geen enkel antivirusproduct in staat al onze virussen te herkennen: naast heel recente ontsnapten ook oudere virussen de virusdetectie. Die alleroudste virussen vormen niet noodzakelijk een probleem voor moderne Windows-systemen. Ze zijn geschreven voor DOS en vanaf Windows 2000 treffen zulke virussen mogelijk niet aan wat ze verwachten en is de kans groot dat ze niet behoorlijk meer werken. Daarom beperken we ons tegenwoordig voor dit soort testen tot onze collectie van EXE-virussen en macrovirussen. We hebben – gemeen als we zijn – een paar 'false positives' of valse positieven apart gezet: een virusdetector krijgt strafpunten als hij die herkent als een virus, want het gaat niet om echte virussen of andere kwaadaardigheden.

Antimalwaretest

Voor de antimalwaretest interesseert ons vooral of de software in staat is een schoon systeem malwarevrij te houden. Daartoe hebben we een doorsnee pc uitgerust met Windows XP en voorzien van Service Pack 2 en alle beveiligings- en andere updates die Microsoft voorschrijft. Op deze pc hadden we ook de gebruikelijke desktopsoftware zoals Microsoft Office met Outlook, Acrobat Reader en dergelijke geïnstalleerd. Als browser was nog steeds IE voorzien, maar Firefox was ook aan boord. Vervolgens installeren we de antimalwaresoftware zoals de producent dat voorschrijft. Daarmee hebben we dus een schoon en goed beveiligd systeem, althans volgens de producent van de beveiligingssoftware en volgens Microsoft. Als normale gebruiker zou je nu gaan rondsurfen en wellicht allerlei dingen uitproberen. Wij zijn redelijk lui en nemen de kortste weg. We downloaden en installeren een op het eerste gezicht leuke gratis mp3-speler: FreeMP3 Player. Dat is, zoals de naam het al aangeeft, een gratis speler voor allerlei geluidsformaten waaronder mp3. Helaas installeert deze gratis speler onder de neus van de gebruiker een waar bataljon aan malware-objecten: daar zitten een paar zéér hardnekkige bij. Als niets de malware tegenhoudt, heeft de

onfortuinlijke pc maar liefst meer dan 400 registerinschrijvingen, meer dan 250 bestanden en ettelijke geheugenlocaties besmet met in totaal een twintigtal malwarefamilies!

Het is uiteraard de bedoeling dat de antimalwareoplossing op deze client-pc alle parasieten tegenhoudt. Hierbij aanvaarden we dat de malwarebestrijder de installatie van de hele mp3-speler tegenhoudt. Als de mp3-speler geïnstalleerd raakt, starten we die uiteraard en proberen een paar dingen uit zoals mp3's afspelen. Pas daarna gaan we controleren hoeveel malware op ons testsysteem aanwezig is. Dat doen we eerst met de te testen antimalwaresoftware. Als die zegt dat er geen malware meer is, controleren we het handmatig. De toegekende testscore is uiteraard afhankelijk van hoeveel malware verwijderd is en hoe gevaarlijk die was. Hoe meer malware we achteraf tijdens onze handmatige controle níét kunnen terugvinden, hoe hoger de score.