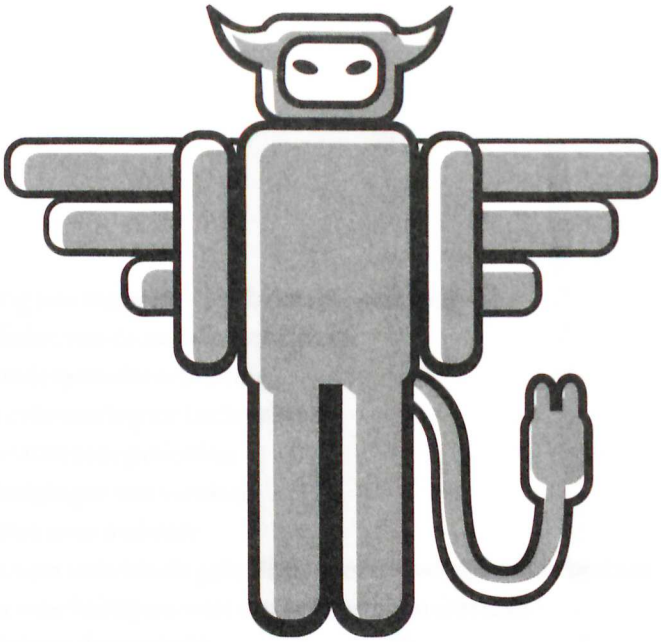
EDDY WILLEMS is een wereldwijd erkende *security specialist*. Hij is *security evangelist* bij de Duitse securitysoftware-leverancier G Data Software en zetelt als directeur in diverse brancheorganisaties, zoals het European Institute for Computer Antivirus Research (EICAR) en AMTSO (Anti-Malware Testing Standards Organization).

CYBER GEVAAR

EDDY WILLEMS



CYBER GEVAAR

HOE WE ONS KUNNEN WAPENEN TEGEN ONLINE MISDAAD... EN MEER

LANNOO

INHOUD

DANKWOORD

Een boek schrijf je nooit alleen, daarom wil ik een aantal mensen hartelijk bedanken.

Nadine, mijn vrouw, verdient een speciale plaats in dit dankwoord. Nadat ik er jaren met haar over gesproken heb, was zij het die de ultieme aanzet gaf om er uiteindelijk mee te beginnen. Zij was mijn niet-technische maar zeer actieve eerstelijns(proef)lezer en ze wilde elk detail goed begrijpen. Daartoe heb ik een aantal hoofdstukken helemaal opnieuw geschreven. Ze was er ook steeds op de momenten dat ze er moest zijn.

Ik bedank Stef Gyssels, een goede vriend en journalist, die me ontzettend geholpen heeft met tientallen stijltips. Hij leerde me dat een boek schrijven toch wel iets anders is dan een blogbijdrage of een interview met de een of andere krant. Het zou mij waarschijnlijk veel meer tijd gekost hebben om dit boek te schrijven zonder zijn positieve inbreng.

Mijn geheime wapen zijn mijn collega's bij G Data geweest: Jan Van Haver en Danielle van Leeuwen. Ik heb geprofiteerd van hun vele kritische opmerkingen. Jan bedank ik voor de goede tips van een boekenkenner en Danielle voor haar research en gedetailleerde stilistische aanvullingen.

Het was erg moeilijk te beslissen welke mensen ik zou vragen om een bijdrage of opiniestukje te schrijven. Ik heb me moeten beperken tot een achttal. Mijn dank gaat uit naar, in alfabetische volgorde: Ralf Benzmüller, Bob Burls, Rainer Fahs, Richard Ford, Natalya Kaspersky, Guy Kindermans, Peter Kruse en Brenno de Winter.

Hopelijk kunnen we samen met dit team de wereld een beetje veiliger maken!

Eddy Willems

INLEIDING

De afgelopen maanden en jaren hebben het nog maar eens onmiskenbaar aangetoond: de tijd dat we onbezorgd konden mailen en surfen behoort definitief tot het verleden. De PRISM-affaire en aansluitend de ontdekking dat de Verenigde Staten ook het online doen en laten volgen van vertegenwoordigers van de Europese Unie in New York en Washington: telkens opnieuw worden we met de neus op de feiten gedrukt: de cyberruimte krioelt van de gevaren en bedreigingen. Ik wil iedereen – jong en oud, IT'er en leek, professional en eindgebruiker – informeren over alle mogelijke online gevaren en waarschuwen voor ongewenst gedrag. Ook wil ik tips geven over hoe je de meeste gevaren kunt voorkomen en schade aan je pc, smartphone of andere apparaten kunt beperken.

Cybergevaar is ruwweg opgedeeld in drie delen. In een eerste deel (hoofdstuk 1 en 2) duiken we de geschiedenis in, van het allereerste virus tot de opmars van de gevaren die ons vandaag de dag bedreigen. In hoofdstuk 2 besteed ik speciale aandacht aan de virusschrijvers: welke types kun je onderscheiden, wat drijft hen, en hoe staan malwarebestrijders tegenover dit toch wel aparte volkje? Dat lijkt misschien minder relevant voor de lezers die vooral willen weten wat hen vandaag bedreigt en hoe ze zich daartegen kunnen wapenen. Maar ik ben ervan overtuigd dat deze inzichten de volgende hoofdstukken helpen begrijpen: je maakt kennis met vele termen die verderop in het boek zullen terugkeren, je krijgt een beter inzicht in de complexiteit van de huidige cyberwereld vol gevaren, en je begrijpt wellicht ook beter waarom zo veel mensen geboeid blijven door alles wat met malware te maken heeft. Met een beetje geluk krijgt de microbe (neen, niet het virus!) ook jou te pakken.

In het tweede deel (hoofdstuk 3 tot 6) krijg je een dieper inzicht in de cybergevaren van vandaag: wie zijn de spelers, wat zijn de bedreigingen, en wie kan je helpen ze te bestrijden? Hoofdstuk 3 duikt in de ondergrondse economie, het werkterrein van de cybercriminelen. Alleen al door de omvang van deze economie, maar ook door de professionele werkwijze waarmee de criminelen te werk gaan en het uitgebreide aanbod aan producten en diensten zal je mond wellicht wijd openvallen. De inhoud van dit hoofdstuk komt voor het grootste deel uit het witboek *The Underground Economy*

dat mijn collega's van de G Data Labs hebben geschreven. Mijn oprechte dank aan hen is hier dus zeker op zijn plaats.

Hoofdstuk 4 benadert de cybergevaren vanuit een andere hoek en bespreekt zij die malware en hacktechnieken om andere dan louter financiële redenen. Meer bepaald komen hier aan bod: cyberspionage, cybersabotage, terrorisme en cyberoorlog (of liever, waarom we niet van 'cyberoorlog' kunnen spreken). Hoofdstuk 5 is gewijd aan de antivirusindustrie: de leveranciers en de organisaties die er alles aan doen om de cybergevaren zo veel mogelijk in te perken. In hoofdstuk 6 gaat het over het cybergevaar van tegenwoordig: welke bedreigingen zien we momenteel als het grootste gevaar voor al wie zich online begeeft, zowat de halve wereld dus.

Het derde deel van dit boek is grotendeels gewijd aan praktisch advies over wat je moet doen en vooral wat je beter niet kunt doen. In hoofdstuk 7 worden eerst een aantal veelgehoorde mythes en misverstanden weerlegd, zodat het voor iedereen duidelijk is waar de echte gevaren schuilen en welke remedies absoluut niet werken. In hoofdstuk 8 staan een hele reeks praktische tips voor iedereen, van de meest voor de hand liggende ('houd je software up-to-date') tot enkele regelrechte verrassingen ('plak je webcam af' of – een van mijn favorieten – 'mediatraining voor iedereen!'). Hoofdstuk 9 is vervolgens specifiek op het bedrijfsleven gericht, met enkele meer gespecialiseerde en soms ook technische tips.

Hoofdstuk 10 en 11 bespreken welke rol de overheid en de media kunnen spelen bij het bestrijden van deze gevaren, en of ze hier altijd even goed in slagen. In hoofdstuk 12 doe ik mijn visie op de nabije toekomst van malware uit de doeken, en hoe we die malware het hoofd kunnen blijven bieden. En als uitsmijter heb ik mijn visie op de verdere toekomst verwerkt in een fictief kortverhaal, waarin ik een aantal voorspellingen voor de cybergevaren anno 2033 heb verwerkt.

Wie dit boek helemaal uitleest, zal zich heel wat beter gewapend voelen om de cybergevaren tegemoet te treden. Daar ben ik van overtuigd. Mijn droom is dat de cybercriminelen en andere 'slechteriken' het dankzij dit boek weer wat moeilijker krijgen om onschuldige slachtoffers in de cyberval te lokken. Laat me vooral weten of ik hier ook in geslaagd ben. Maar ik wens je ook veel leesplezier bij het ontdekken van alle gevaren. Een goede thriller mag niet saai zijn, en ik hoop dat dit boek ook op dat vlak een goede thriller zal blijken. Maar zal ik eerst mezelf even voorstellen?

GA JE MET ME MEE?

Wie ooit een georganiseerde reis heeft meegemaakt, weet waarover ik spreek: het is altijd leuker als de gids zich even voorstelt. Wie is hij, waar komt zij vandaan, wat geeft hem het recht om de komende veertien dagen te beslissen waar we naartoe gaan, wat we te weten komen over onze bestemming en over de vele wonderbaarlijke zaken die we onderweg nog tegenkomen? Pas als je het gevoel hebt dat je de gids een beetje kent, ben je bereid om helemaal mee te gaan in zijn of haar verhalen.

Daarom lijkt het me verstandig dat ik me ook even voorstel. Je gaat per slot van rekening niet met eender wie scheep voor een hopelijk lange reis door de wereld van het cybergevaar. Na het lezen van deze inleiding heb je er hopelijk ook vertrouwen in dat je als je deze reis met mij aanvat, behouden terug zult keren. En dat het een reis is die je zal boeien en verrassen, en af en toe misschien ook choqueren, maar dat het ten slotte een tocht is die je wijzer en voorzichtiger maakt, in de wetenschap dat het cybergevaar om elke hoek kan loeren.

EEN JEUGD VOL TECHNOLOGIE

Ik ben opgegroeid in Mechelen, als zoon van een winkeliersgezin. De secundaire (middelbare) school in Mechelen was waarschijnlijk een van de eerste in België die lessen informatica aanbood aan haar leerlingen. Die eerste cursussen gingen vooral over programmeren in eenvoudige talen, zoals Basic. Niets spectaculairs dus, maar wel voldoende om mijn interesse te wekken.

Programmeren werd meteen mijn grootste hobby, naast experimenteren met elektronicadozen, scheikundige projecten en radioamateurisme (destijds ook wel bekend als CB of 27 MC) in al zijn aspecten, zowel de technische als de communicatieve.

In 1980 was informatica nog een geheel nieuwe studierichting. De universiteiten waren nog volop bezig om deze academische opleiding in te vullen, en ze wisten nog niet goed hoe ze ermee moesten omgaan. Ik koos eerst voor computerwetenschappen aan de Vrije Universiteit Brussel en daarna voor wat nu de Erasmushogeschool is. Daar lag de nadruk op het leren van programmeertalen zoals Pascal, Assembler en Fortran, wat meer plezier dan een opgave was.

In die periode werkte ik ook bij de zogeheten 'vrije radio', als technische man achter de schermen. Een aangename periode, waar ik ook heel wat bijleerde over het belang van helder communiceren voor een groot publiek.

EERSTE ERVARING, EERSTE PC

Na mijn studies vond ik onmiddellijk een baan als programmeur bij een groothandel in voedingswaren. Ik mocht werken met Cobol op een grote machine van Bull. Een leuke ervaring, dat wel, maar al vrij snel begon ik me te ergeren aan de gebruiksonvriendelijkheid van dat toestel: net als bij de meeste mainframes en andere servers uit die tijd moest je werken op zwarte schermen met groene tekens. Bovendien vond ik die grote apparaten ook helemaal niet handig: je kon die niet eens mee naar huis nemen! Het verklaart mijn enthousiasme toen in ons bedrijf de eerste IBM-pc werd binnengebracht: een 'draagbaar' apparaat waarop je ook in Cobol kon programmeren, met daarin een harde schijf van maar liefst 5 MB. Die zou ik toch nooit vol krijgen, dacht ik toen. Ik zag meteen het potentieel van deze apparaten. Het duurde nog enige tijd voor ook mijn collega's hiervan overtuigd raakten, maar ik wist toen al dat mijn toekomst parallel zou lopen met die van deze persoonlijke computers.

Toen ik in 1987 toe was aan een nieuwe uitdaging, vond ik die bij de (toenmalige) Vaderlandsche Verzekeringen (een onderdeel van Nationale Nederlanden, nu ING). Bij de Vaderlandsche kon ik mijn twee grootste passies in één baan verenigen: als helpdeskmedewerker kon ik de voldoening smaken om mensen uit de problemen te halen, maar ik mocht ook software ontwikkelen om de helpdesk beter te laten functioneren. Tegelijk kregen we ook de kans om aan zelfstudie te doen en nieuwe programma's uit te testen, waar ik dankbaar gebruik van maakte om mijn softwarekennis te verbreden.

In 1989 kreeg ik, zoals zo vaak, een programma toegeschoven om te evalueren of het iets voor het bedrijf kon zijn. Het was een diskette die met een informaticaboekje was meegeleverd, met een programma erop waarmee je kon vaststellen of je tot de risicogroep behoorde die aids kon krijgen. Het programma bleek een sof, en ik vond het heel gek dat ze zoiets met een ICT-boekje meestuurden.

Maar de volgende dag hadden we de poppen aan het dansen. Ik startte mijn pc en er gebeurde helemaal niets. Er was enkel een scherm te zien waarop stond dat je geld moest storten op een bepaald rekeningnummer. Ik herstartte de pc, en toen gebeurde er helemaal niets meer. Ik dacht dat er een bug in zat. Toen startte ik maar op vanaf een systeemdiskette en zag waar de 'fout' zat: het pad was veranderd en versleuteld... zonder het te beseffen had ik kennisgemaakt met de eerste 'ransomware', programma's ontwikkeld om je pc te gijzelen en slechts na betaling weer vrij te laten.

Niettemin had ik het probleem in enkele minuten omzeild en konden we ongehinderd voortwerken.

Groot was dan ook mijn verbazing toen ik twee dagen later op het journaal van de nationale commerciële zender VTM hoorde vertellen dat deze ransomware de ronde deed 'en geen enkel bedrijf heeft een oplossing'. Huh, geen enkel bedrijf? Ik had dat toch eergisteren opgelost? Dus belde ik het VTM-journaal om te vertellen dat ik dat probleem wel had omzeild, zonder veel moeite zelfs. De volgende dag stond een cameraploeg bij me thuis en het resultaat viel 's avonds op het journaal te bewonderen.

DE MALWARETREIN WAS VERTROKKEN

Om in malwareterminologie te blijven: het Aids-virus had me besmet. Ik besefte dat dit was wat ik eigenlijk altijd had willen doen: het ontdekken en in kaart brengen van virussen en zoeken naar manieren om ze te bestrijden. Ik ging, via bulletinboards, op zoek naar mensen en organisaties die zich ook met virussen bezighielden. Zo ontdekte ik bedrijven als McAfee en Dr. Solomon's, maar ook interessante persoonlijkheden zoals dr. Sarah Gordon (zie ook blz. 39).

Zo werd ik in 1991 ook uitgenodigd voor een conferentie over virusbestrijding in Brussel. Daar waren alle grote namen uit dat wereldje aanwezig: dr. Solomon zelf, Vesselin Bontchev en vele anderen. Ik was er zeker van: dit zou meer dan een hobby moeten worden, hier moest ik mijn beroep van maken. Tijdens die conferentie werd ook EICAR opgericht, en ik kan me dus met enige trots stichtend lid van deze organisatie noemen.

Gelukkig waardeerde men bij De Vaderlandsche mijn interesse voor virussen en de programmeerervaring die ik hiermee verwierf, zodat ik mijn passie ook professioneel kon benutten. Intussen maakten de bulletinboards plaats voor e-mail en websites. Al was dat in het begin allesbehalve gemakkelijk: na een lange zoektocht naar de juiste software om te browsen en een urenlang configuratiegevecht was ik eindelijk klaar om te surfen... om vervolgens te ontdekken dat er online nauwelijks iets te vinden was!

Over virussen en andere vormen van malware was er dus helemaal bijna niets te vinden. Zelfs bedrijven als McAfee kon je in 1994 niet online vinden. Daarom besloot ik zelf een site te wijden aan virussen. Deze site, www.wavci.com, bevatte links naar andere sites, voorbeelden van virussen en andere nuttige informatie. Ik wilde als het ware een online antivirusencyclopedie maken. Dat trok de aandacht van heel wat beveiligingsspecialisten. Mede daarom werd ik voor heel wat evenementen uitgenodigd. Zo ook voor

de Virus Bulletin-conferentie in Brighton in 1996, waar ik Harry De Smedt ontmoette. Harry was manager van Data Alert, de afdeling van Unit 4 die zich richtte op beveiligingssoftware: zij distribueerden Dr. Solomon's Antivirus Toolkit, destijds een van de meest gewaardeerde antiviruspakketten. Door mijn onlineactiviteiten kende Harry De Smedt mij al vrij goed, en voor ik het besefte kreeg ik een aanbieding om bij hen te gaan werken.

Zo begon ik op 1 januari 1997 bij de toenmalige beveiligingsdienstenleverancier en -distributeur Data Alert. Sindsdien heb ik zowat alle antivirusconferenties bijgewoond. Aan die van Virus Bulletin geef ik verreweg de voorkeur: alle belangrijke personen zijn daar aanwezig, en er is dus geen betere plek om informatie te vergaren en je netwerk uit te breiden. Ook de conferenties van EICAR en CARO zijn zeer aanbevelenswaardig. Als ik maar enkele conferenties per jaar mocht bezoeken, zouden het deze drie zijn.

Data Alert werd na enkele jaren (en overnames) NOXS, de beveiligingspijler binnen Unit 4 Agresso, dat onder de naam UNIT4 nog steeds een belangrijke ICT-leverancier is op de zakelijke markt. Via een heleboel omwegen kwam ik in die jaren in contact met de allergrootsten binnen de antiviruswereld: Sarah Gordon, Righard Zwienenberg, dr. Solomon, Mikko Hyppönen en anderen. Zo werd ik ook lid van het Vforum, een vriendenclub van virusexperts waar je enkel op uitnodiging binnenkomt, en waar alle bekende namen uit de industrie lid van zijn.

De antivirusgemeenschap is een zeer hechte groep. Tussen antivirusleveranciers bestaat een grote solidariteit en bereidheid om kennis over malware te delen. Ikzelf liet me bijvoorbeeld niet onbetuigd in het in kaart brengen van virussen, alleen al omdat ik bij zo veel ondernemingen 'in het veld' malware kon opsporen.

Mijn taak binnen NOXS bestond vooral uit research, consultancy en opleidingen bij alle klanten. NOXS, dat later is opgegaan in Westcon Security, groeide intussen ook uit tot een grotere organisatie met een zekere reputatie. Zo kwam ik over de vloer bij meer dan duizend organisaties, van kleine tot de allergrootste, inclusief alle Belgische overheidsdiensten. Ik moest ook vaak projecten begeleiden in het buitenland, vaak niet bij de minste klanten (zoals je kunt lezen in het kader 'No problem in Saudi Arabia' op blz. 16). En als ik iets niet kon oplossen, kon ik altijd terecht bij iemand uit mijn 'rode boekje' met contacten bij de meeste grote leveranciers die ik letterlijk dag en nacht kan bellen. Het (menselijke) netwerk is in de beveiligingswereld zeker even belangrijk als de kennis van alle malware.

In 2000, ten tijde van het 'Love letter'-virus, besloot de overheid, in de persoon van toenmalig minister van Telecommunicatie Rik Daems, een soort van antimalwarecel op te richten, 'in nauw contact met de privésector'. Toen ik dat 's avonds op de televisie hoorde verkondigen, borrelde een gevoel van verontwaardiging op. Hoe konden ze beweren dat de privésector nauw betrokken was terwijl er geen enkele vertegenwoordiger uit de privésector zelfs maar werd geconsulteerd? Met die verontwaardiging stapte ik naar VTM, die hier gretig op inging, wat leidde tot mijn tweede verschijning in het journaal. Gelukkig leidde het ook tot concrete samenwerking, en zo raakte ik betrokken bij een cel binnen de overheid die aan malwarebestrijding deed, een voorloper van het huidige Computer Emergency Response Team (CERT) eigenlijk. In het begin liet deze cel af en toe op de openbare omroep waarschuwingen uitsturen voor gevaarlijke virussen en andere computerbedreigingen. Een soort van digitaal verkeersbericht, zeg maar: 'Het is opletten geblazen voor een nieuw virus...' Paniek was niet nodig maar voorzichtigheid was wel geboden. Nu nog trouwens.

In die periode was ik soms de officieuze woordvoerder van die cel, wat leidde tot tientallen interviews. En ik adviseerde deze cel over de malware die werd gevonden: was het belangrijk, was het een hoax, moest de bevolking worden gewaarschuwd? Het was een zeer actieve cel, veel actiever dan het huidige CERT.

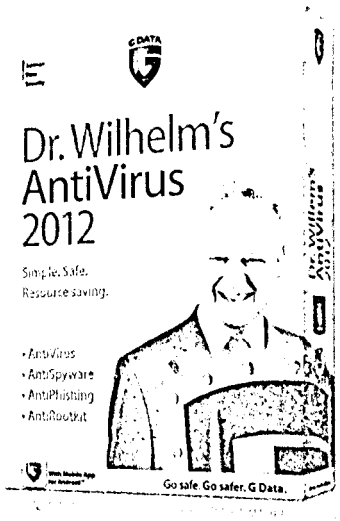
DE EVANGELISTENJAREN

NOXS vormde jarenlang een sterk team van beveiligingsexperts, waarvan de meesten ook nu nog hoge functies in de beveiligingswereld bekleden. Het was een plezier om met dit team jarenlang de cybermisdaad te bevechten. Maar elk liedje, hoe mooi ook, kent een einde.

Eind 2007 koos ik voor Kaspersky Lab, een bekende leverancier van antimalwaresoftware, omdat ik daar niet alleen met research bezig kon zijn, maar ook met het uitleggen en verspreiden van de blijde antimalwareboodschap. Vanaf toen was ik een Kaspersky-evangelist binnen het Kaspersky expertenteam, die enerzijds kon uitleggen waarin de concurrentie faalde en anderzijds bij het grote publiek kon blijven hameren op het belang van beveiliging. Een taak waar ik me tot vandaag toe geregeld in uit kan leven.

Enkele jaren later kreeg ik de gelegenheid om bij het Duitse antivirusbedrijf G Data te beginnen. Een aanbod dat ik niet kon weigeren, met nog meer mogelijkheden om me te ontwikkelen en de vinger aan de pols te houden. Dus heb ik begin 2010 de overstap gemaakt, en daar heb ik nog

geen moment spijt van gehad. Zeker niet nadat ik mocht proeven van de uitstekende sfeer, waarin er niet alleen plaats is voor hard werken maar waar ook af en toe hard wordt gelachen. Een mooi voorbeeld hiervan is deze illustratie waarin ze een 'Dr. Wilhelm'-editie van onze software hadden gemaakt. Voor wie daaraan mocht twijfelen: dit is puur PhotoShop-werk, er is nooit een dergelijke editie geweest.



Sinds maart 2001 zit ik ook in de raad van bestuur van antivirusorganisatie EICAR, waar ik nu directeur Security Industrie Relaties ben. Met mijn activiteiten voor EICAR en AMTSO (een andere wereldwijde beveiligingsorganisatie, die ik net als EICAR in een later hoofdstuk uitvoerig behandel) enerzijds en mijn fulltimebaan bij G Data anderzijds merk ik dat ik precies heb bereikt waar ik met mijn carrière heen wilde: veel ruimte voor de technische kant, maar ook veel aandacht voor de menselijke factor, in het besef dat ik in mijn rol ook echt mensen kan helpen. Mijn grote hoop met dit boek is dat ik er uiteindelijk ook jou mee zal hebben geholpen.

DISCLAIMER

Nog even dit, voor we echt van start gaan. Ook al werk ik al vele jaren in een internationale context, toch zullen verschillende voorbeelden en anekdotes een Belgische context hebben. Niettemin heb ik enkel die voorbeelden gekozen die ook voor lezers uit andere landen relevant zijn. Het uitgangspunt is steeds geweest: wat kan de lezer van een boek over cybergevaar interesseren, ongeacht zijn nationaliteit of haar woonplaats.

Hetzelfde geldt voor grafieken, schema's en cijfers die in dit boek worden gebruikt. Omdat ik bij antivirusleverancier G Data werk, heb ik veel materiaal van dit bedrijf tot mijn beschikking. Maar ik ben ervan overtuigd dat deze cijfers en het andere materiaal grotendeels overeenkomen met waar andere leveranciers over beschikken. Ook hier geldt: het belang van de lezer staat