Opinie

Wet computercriminaliteit

Onvoorziene consequenties

Mw. Mr. A.M.Ch. Kemna
en Prof. A.W. Neisingh

De Wet computercriminaliteit (WCC),[1] die per 1 maart 1993 van kracht is geworden, bevat in tegenstelling tot de Wet persoonsregistraties (WPR) geen beveiligingsplicht,[2] zo wordt wel aangenomen. Naar onze mening is deze aanname onjuist en kan zij voor cliënt en accountant tot onvoorziene complicaties leiden. Er wordt ingegaan op de impliciete beveiligingsplicht voortvloeiend uit de artikelen 161septies Sr. en 350b Sr. De voorziene consequenties voor accountants en EDP auditors worden vanuit deze invalshoek nog eens bekeken. Voorts wordt aangegeven wat de reikwijdte is van de nieuwe delictsomschrijvingen en hun onderlinge verhouding.
Bedoeling van deze bijdrage is onder vakgenoten een discussie op gang te brengen.

De WCC in het kort

De Wet computercriminaliteit, kortweg WCC, heeft in zijn nog maar korte leven reeds veel publiciteit gekregen. De hoofdlijnen van de wet mogen dan ook inmiddels genoegzaam bekend worden geacht.[3] Een korte samenvatting: de WCC is onder meer gebaseerd op het rapport 'Informatietechnologie en Strafrecht' van de eerste Commissie Franken uit 1987. De Commissie hechtte grote waarde aan het bevorderen van het beveiligingsbewustzijn bij overheid en bedrijfsleven in het kader van de voortschrijdende automatisering en informatisering van het maatschappelijk leven. Haar verontrusting was op dit punt onder meer gewekt door een onderzoek dat zij liet uitvoeren naar de stand van de beveiliging van informatietechnologie in Nederland.[4]
De huidige wetstekst bevat een groot deel van de aanbevelingen van de Commissie Franken. De wijzigingen in het Wetboek van Strafrecht zijn er op gericht bepaalde handelingen in een geautomatiseerde omgeving strafbaar te stellen. Bekende voorbeelden van strafbare gedragingen zijn het verspreiden van virussen en het *'hacken'*: het opzettelijk wederrechtelijk binnendringen in een geautomatiseerd werk dat ofwel daartegen is beveiligd ofwel doordat de *hacker* een 'valse hoedanigheid' aanneemt of 'valse sleutels' gebruikt (andermans *user-ID* en *password*) [5] Wijzigingen in het Wetboek van Strafvordering zijn bedoeld om politie en justitie faciliteiten te bieden ten behoeve van opsporing en vervolging in een dergelijke omgeving.

Mr. A.M.Ch. Kemna MBA is werkzaam bij KPMG Klynveld EDP Auditors als adviseur informaticarecht en is voorts onderzoeker bij de afdeling Recht & Informatica, Juridische Faculteit, Rijksuniversiteit Leiden.

Prof. A.W. Neisingh RE RA is vennoot van de maatschap KPMG Klynveld EDP Auditors en voorts hoogleraar betrouwbaarheidsaspecten van geautomatiseerde informatiesystemen bij de vakgroep Accountancy, Economische Faculteit, Rijksuniversiteit Groningen.

De wijziging van artikel 2: 393 lid 4 BW tenslotte verplicht de controlerend accountant bij het verslagleggen aan het bestuur en de Raad van Commissarissen omtrent zijn onderzoek in het kader van de jaarrekening 'ten minste melding te maken van zijn bevindingen met betrekking tot de betrouwbaarheid en de continuïteit van de geautomatiseerde gegevensverwerking'. Dit artikel is wellicht een wat vreemde eend in de bijt, doch is bezien in het licht van bovengenoemde bevindingen van de Commissie Franken zeer wel verklaarbaar.

Nieuwe 'culpose delicten'

Een minder bekend en beschreven aspect van de WCC is het volgende.
Tijdens de behandeling van de WCC in de Tweede Kamer is een amendement aanvaard dat tot een opmerkelijk neveneffect heeft geleid. Er zijn twee geheel nieuwe strafbaarstellingen van 'culpose delicten' toegevoegd. Dat zijn strafbepalingen die niet op *opzet* van de dader zien, maar op diens *schuld* aan een bepaalde strafbare gedraging of gebeurtenis.[6]
De beide delictsomschrijvingen richten zich specifiek op handelingen en/of omissies in geautomatiseerde omgevingen. Het betreft de bepalingen 350b (schuld aan manipuleren van gegevens onder meer door virussen) en 161 septies (schuld aan verstoring van gegevensverwerking) Wetboek van Strafrecht.[7]
Ten gevolge van deze bepalingen is men nu bijvoorbeeld strafbaar, indien het aan schuld te wijten is dat strafbare handelingen en ongewenste gebeurtenissen hebben kunnen plaatsvinden. Bij 'schuld' dient het conform vaste jurisprudentie volgens de Memorie van Toelichting[8] te gaan om een min of meer grove of aanmerkelijke onvoorzichtigheid, onachtzaamheid of nalatigheid. Indien door het management van een organisatie onvoldoende aandacht is besteed aan maatregelen van interne controle en beveiliging, kan zo strafbaarheid ontstaan indien daardoor een virus zich kan verspreiden en schade aan de programma's en gegevens (al dan niet van anderen!) aanricht. Nog groter zou de schade kunnen zijn indien er een externe verbinding is. Cliënten of leveranciers 'lopen een virusbesmetting op'. Door onvoldoende toegangsbeveiliging verschaffen ongeautoriseerde personen zich een weg tot gegevens of veroorzaken schade aan de gegevensverwerking. Naast een civielrechtelijke aansprakelijkheidsstelling (en wellicht problemen met de verzekering) zou het management van een organisatie in zo'n geval dus bovendien strafrechtelijke problemen kunnen verwachten!

Reikwijdte en onderlinge verhouding

Wat is nu precies de reikwijdte van de nieuwe schulddelicten uit de WCC? Voor welke organisaties zijn zij van belang?
De kans dat de artikelen 350b en 161septies Sr. in een concreet geval van toepassing zouden kunnen zijn, zal onder meer afhankelijk zijn van de aard van de automatisering. Maar er zijn meer omstandigheden. De beide artikelen geven de randvoorwaarden voor de benodigde risico-inschatting (zowel voor de organisatie zelf als ten behoeve van de Officier van Justitie):
Volgens artikel 161 septies moet het gaan om personen of organisaties die gebruik maken van systemen (ook telecommunicatie) waardoor of waarbij, indien het systeem wordt 'vernield, beschadigd of onbruikbaar gemaakt', of indien 'stoornis in de gang of in de werking ontstaat', of indien 'een ten opzichte van zodanig werk genomen veiligheidsmaatregel wordt verijdeld', één (of meer) van deze gevolgen zouden kunnen optreden:
- verhindering of bemoeilijking van opslag en of verwerking van gegevens ten algemenen nutte;
- stoornis in de telecommunicatie-infrastructuur (bedoeld is hier de openbare, red.);
- gemeen gevaar voor goederen of voor de verlening van diensten;
- levensgevaar voor een ander;
- iemands dood.

Artikel 350b Sr. geldt vervolgens niet alleen ten aanzien van de voorgaande personen en organisaties, maar voor alle personen en organisaties:
- aan wiens schuld het is te wijten dat ernstige schade aan geautomatiseerde gegevens ontstaat door manipulatie van die gegevens, op welke wijze ook (al dan niet door een virus), of
- aan wiens schuld het is te wijten dat een virus zich kan verspreiden dat schade (in welke vorm of mate ook) aanricht of aan kan richten.

De beide artikelen samengevat:
- als een virus door schuld (grove onachtzaamheid, nalatigheid) verspreid wordt kan de betreffende (rechts-)persoon altijd strafbaar zijn, mits het virus bedoeld is om schade aan te richten (wat voor schade ook, bij wie dan ook); de strafmaat is ten hoogste een maand of een vergelijkbare geldboete;
- als door bijvoorbeeld dat virus of door andere manipulatie daadwerkelijk ernstige schade aan gegevens (van wie dan ook) ontstaat is de schuldige eveneens strafbaar, de strafmaat is ook dan een maand of een vergelijkbare geldboete;
- als die manipulatie of dat virus of enige andere (al dan niet als saboterend bedoelde) handeling door middel van of ten nadele van het systeem van de schuldige de nog ernstiger schadevormen ten gevolge heeft als bedoeld onder artikel 161septies (aan of door zijn systeem of aan of door dat van een ander), dan is de strafmaat drie maanden of een boete van *f* 25.000, respectievelijk zes maanden of een boete van *f* 25.000, respectievelijk een jaar of een boete van *f* 25.000.

Wanneer is er schuld?

Opgemerkt zij, dat de daadwerkelijk schadeveroorzakende handeling door een ander uitgevoerd kan zijn; de schuld betekent dat de persoon of de organisatie in kwestie het had moeten (kunnen) voorkomen of beter had moeten weten.
Wanneer er in een geautomatiseerde omgeving sprake is van 'schuld', 'aanmerkelijke onvoorzichtigheid of nalatigheid', en wanneer bijvoorbeeld een virus is 'bedoeld om schade aan te richten', of wanneer er sprake is van 'ernstige schade', of 'gemeen gevaar', zal onder meer gaan afhangen van de interpretatie die de rechter aan deze artikelen gaat geven. Wel valt nu al op dat er sprake is van gradaties: de strafmaat wordt hoger naarmate het gevolg ernstiger is of zal zijn. Iedereen dient zijn computersysteem te beveiligen tegen virussen, maar een organisatie die ernstige(r) schade kan veroorzaken moet nog meer doen. Er dient dus een duidelijke afweging gemaakt te zijn door degene op wie de bepalingen van toepassing zouden kunnen zijn: indien er iets gebeurt door of met het systeem dan wel de gegevens van een bepaalde organisatie, welke gevolgen zou dat kunnen hebben en welke schade kan dan optreden. Aan de hand daarvan dient bepaald te worden welke maatregelen getroffen dienen te worden.
Het feit dat er sprake moet zijn van 'grove of aanmerkelijke schuld' geeft aan, dat eveneens gekeken wordt naar de soort organisatie, de soort dienstverlening dan wel de kennis of ervaring van een dergelijke organisatie. Als extreem voorbeeld: je als ziekenhuis beroepen op onwetendheid van bepaalde risico's in automatisering van patiënten-, respectievelijk medicijnenregistraties lijkt een niet echt zinvolle actie. Men spreekt van 'geobjectiveerde schuld'. Men kijkt dan voor het beoordelen van de schuld naar hetgeen van vergelijkbare personen/organisaties over het algemeen verwacht mag worden.

Adequate beveiligingseis

Waar risico aanwezig is dienen er in ieder geval aantoonbare beveiligingsmaatregelen getroffen te zijn. Dat is echter naar onze mening nog niet voldoende. De aantoonbaarheid levert een ontegenzeglijk bewijsvoordeel, ech-

ter er blijkt nog niet uit dat er de bovengenoemde adequate afweging is gemaakt (ofwel: 'aantoonbaar' kan zowel inhouden 'minimaal' als 'adequaat' als 'maximaal'; het geeft nog geen waarde-indicatie). Er dient naar onze mening tevens sprake te zijn van afweging van de aard van de risico's en een bewuste keuze van de in dat kader te treffen beveiligingsmaatregelen. En daarmee zijn wij aangeland bij de expliciete beveiligingseis in de Wet persoonsregistraties, waarin eveneens een adequate beveiliging geëist wordt, maar dan specifiek ten aanzien van persoonsgegevensbestanden in het kader van betrouwbaarheid, continuïteit en voorts vertrouwelijkheid: evenwicht tussen te beschermen belangen en te nemen maatregelen. Wij merken ten overvloede op, dat de WPR bovendien een (civielrechtelijke) risicoaansprakelijkheid introduceert ten gunste van gedupeerde geregistreerden(9). Dat komt dus nog eens boven op de strafbaarheidsrisio's uit de WCC en overige contractuele en niet-contractuele civielrechtelijke aansprakelijkheden van organisaties in verband met geautomatiseerde gegevensverwerking.

Beveiligingsbeleid en risicobewustzijn

Nog wat verder voortbordurend op artikel 161septies Sr.: het enkele treffen van aantoonbare adequate beveiligingsmaatregelen is nog niet voldoende, er dient ook sprake te zijn van beheer daarvan. Cfr. de zinsnede uit artikel 161septies Sr.: 'indien een ten opzichte van zodanig werk genomen veiligheidsmaatregel wordt verijdeld'. Dat kan natuurlijk altijd want absolute beveiliging bestaat er voor zover schrijvers bekend nog steeds niet. Maar als het aan iemands schuld te wijten is, bijvoorbeeld omdat beveiligingsmaatregelen slecht afgewogen genomen zijn, of ook omdat het treffen van maatregelen als eenmalige actie werd gezien ('hierbij zij er voortaan beveiliging'), dan kan artikel 161septies Sr. mogelijk weer om de hoek komen kijken. Een voortdurend beleid/proces binnen de organisatie is nodig in verband met dit artikel. En daarmee zijn wij teruggekeerd bij de Commissie Franken en één van haar 'grondgedachten': door middel van de WCC dient mede het beveiligingsbeleid en risicobewustzijn binnen geautomatiseerde organisaties gestimuleerd te worden.

Consequenties

Het is de vraag of de wetgever de 'beveiligingsplicht via de achterdeur' in al haar consequenties heeft doordacht. Nu de wet echter in deze vorm van kracht is geworden, dient er een passend antwoord op gevonden te worden. Dit geldt niet alleen voor geautomatiseerde organisaties (en welke organisatie is dat tegenwoordig niet?) maar ook voor de accountants van die organisaties, die zich volgens bovengenoemd artikel 2: 393 lid 4 BW in voorkomende gevallen met de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking dienen bezig te houden. Bepalen zij (en zo ja: hoe?) of de risico's uit deze 'schuldvarianten' in de WCC afdoende binnen een organisatie zijn afgedekt? Realiseren zij zich hun eigen risico's in dit kader indien zij de keuze maken al dan niet gevolg te geven aan artikel 2: 393 lid 4 BW bij een bepaalde organisatie?
Het verdient naar onze mening aanbeveling in meldingen ter voldoening aan artikel 2: 393 lid 4 BW gewag te maken van dit aspect van de WCC. Indien accountants in het kader van de uitvoering van de controle van de jaarrekening op enigerlei wijze de automatisering zouden beoordelen menen wij voorts dat inzet van EDP Auditors in het kader van de uitvoering van die controle van groot belang is.

Noten

1 Wet van 23 december 1992 tot wijziging van het Wetboek van Strafrecht en van het Wetboek van Strafvordering in verband met de voortschrijdende toepassing van informatietechniek (Wet computercriminaliteit).
2 Artikel 8 Wet persoonsregistraties: 'De houder (van een persoonsregistratie, AWN) draagt zorg voor de nodige

voorzieningen van technische en organisatorische aard ter beveiliging van een persoonsregistratie tegen verlies of aantasting van de gegevens en tegen onbevoegde kennisneming, wijziging of verstrekking daarvan. Gelijke plicht rust op de bewerker (bijvoorbeeld een extern salarisbureau, AWN) voor het geheel of het gedeelte van de apparatuur die hij onder zich heeft.'
N.B.: Het niet voldoen aan deze plicht brengt een risicoaansprakelijkheid met zich mee voor de houder (ook voor gedragingen van de bewerker).
3 Zie voor een uitgebreide analyse ook: R.A. s'Jacob, 'Strafbaarstelling van computermisbruik. Een analyse van de Wet computercriminaliteit.' in: *Twintig over Informatietechnologie en Recht*, red. A.M.Ch. Kemna en A.W. Neisingh, Samsom Bedrijfsinformatie/KPMG Klynveld EDP Auditors, 1993.
4 Informatietechniek en Strafrecht, Staatsuitgeverij, Ministerie van Justitie, 1987, pag. 97 e.v. en Bijlage D: Rapport uitgebracht aan de Commissie Computercriminaliteit inzake beveiligingsmaatregelen tegen computercriminaliteit, 15 december 1986, KMG Klynveld Kraayenhof & Co (KPMG).
5 Artikel 138a Sr.
6 Voor de niet-Latinisten: *culpa* is Latijn voor *schuld*.
7 Artikel 161septies Sr.: 'Hij aan wiens schuld te wijten is dat enig geautomatiseerd werk voor opslag of verwerking van gegevens of enig werk voor telecommunicatie wordt vernield, beschadigd of onbruikbaar gemaakt, dat stoornis in de gang of in de werking van zodanig werk ontstaat, of dat een ten opzichte van zodanig werk genomen veiligheidsmaatregel wordt verijdeld, wordt gestraft ..... (enz).
Artikel 350b Sr. Lid 1: 'Hij aan wiens schuld te wijten is dat gegevens die door middel van een geautomatiseerd werk zijn opgeslagen, worden verwerkt of overgedragen, wederrechtelijk worden veranderd, gewist, onbruikbaar of ontoegankelijk gemaakt, dan wel dat andere gegevens daaraan worden toegevoegd, wordt, indien daardoor ernstige schade met betrekking tot die gegevens wordt veroorzaakt, gestraft met..... . Lid 2: 'Hij aan wiens schuld te wijten is dat gegevens wederrechtelijk ter beschikking gesteld of verspreid worden die bedoeld zijn om schade aan te richten door zichzelf te vermenigvuldigen in een geautomatiseerde werk, wordt gestraft met .....'.
8 MvT pag. 19.
9 Artikel 9 WPR.