

Henk-Jan van der Molen

# Open einde

*Alles in deze tekst is fictie, behalve de feiten over Open Standaarden.*

2016, 19 DECEMBER 05:25

**Van Woustraat, Amsterdam**

“AT in positie” klinkt het blikerig in de beveiligde intercom. De springstofexpert van het arrestatieteam kruipt behoedzaam onder het raam door en plakt snel het slagkoord vast aan het deurkozijn. De twee agenten aan weerskanten van de deur pakken elk een flashbang. Het is pikdonker in de straat, vanwege het door de politie ‘geplande’ onderhoud aan de straatverlichting. Met hun *enhanced vision* brillen zien de teamleden hun leider drie vingers opsteken, dan twee, één en dan zwaait zijn arm omlaag. Bijna tegelijkertijd valt met een droge knal de deur inclusief kozijn plat op het trottoir. “Go, Go, GO!” Met hun Heckler & Koch wapens in aanslag golft het arrestatieteam als een waterval naar binnen. Twee oogverblindende flitsen met harde knallen volgen. Uit de woning klinkt op verschillende plaatsen “Police! Show me your hands!” en kreten van woede en angst. In één kamer gaat het schreeuwen door, totdat er twee schoten klinken.

“Onder controle” hoort de leider AT in zijn oor. “Gewonden?” vraagt hij gespannen. “Eén arrestant licht gewond, geen ambulance nodig.” In verschillende woningen in de buurt gaan de lichten aan. De leider geeft opdracht de arrestanten geboeid en geblinddoekt af te voeren naar separate locaties. “Opschieten! Ik wil weg voor de pers er is. En geen fouten, de politiek kijkt vandaag mee.”

20 DECEMBER 09:24

**Geheime locatie in Amsterdam-Zuidoost**

Buiten waait de sneeuw tegen de geblindeerde ramen. Binnen hangt een verstofte spaarlamp aan het plafond en tikt de oude verwarming. Commissaris Peter Both van het Korps Nationale Politie wacht op de laatste verdachte. De arrestatie gisteren was de kroon op het lange onderzoek van het Team High Tech Crime binnen het KNP. Het Nationaal Cyber Security Centrum had overigens het leeuwendeel bijgedragen aan de arrestatie van de bende gisteren. Maar er waren ook dingen grandioos misgegaan.

De politie kreeg begin vorig jaar een tip dat de cyberbende elke week in Amsterdam steeds in ander Indiaas restaurant ging eten. Na een streng geheim gehouden onderzoek volgde een spectaculaire inval in het restaurant Taj Mahal. Toen bleek dat de ‘tip’ niet waar was, had de pers de bende daarna Cash & Curry genoemd. Kort daarna had Peter onverwacht het commando gekregen over de cybercrime unit en de leiding over het onderzoek naar deze bende.

“Peter!” Hij schrikt op uit zijn mijmeringen en kijkt Chris de Vries aan, die als digitaal rechercheur deels werkt bij het Nationaal Cyber Security Centrum. Ze knipoogt. “Lange dag gehad? Wil je zo meteen zijn dossier erbij?”

Peter rekt zich geeuwend uit. “Nog niet. Tot dusver heeft geen enkele verdachte iets losgelaten. Deze arrestant heeft speciaal naar de leider van het onderzoek gevraagd. Ik wil eerst horen wat hij te zeggen heeft.”

De arrestant wordt binnengereden in een rolstoel, snurkend met een rappend geluid. Met handboeien om zijn polsen en een provisorisch verband om zijn linker kuit, waar hij werd getroffen door een politiekogel. De leider van het arrestatieteam had verklaard dat de man weigerde zijn wapen neer te leggen.

Chris maakt aanstalten om de verdachte te wekken. “Voorzichtig!” zegt Peter. Chris antwoordt rustig: “Zwarte band judo” en schudt aan zijn schouder. Geen reactie, zelfs na nog een keer schudden gaat het snurken door. De lachrimpels van Peter verdiepen zich. “Chris, als jij eens een emmer water gaat halen”. Even later komt ze terug met een prullenbak half gevuld met water. Op dat moment houdt het snurken abrupt op en gaat de man rechtop in zijn rolstoel zitten. Hij opent zijn ogen en kijkt Peter direct aan.

Peter start de recorder, zegt de datum en tijd en vraagt “Who are you? Wie ben je?” De man antwoordt in vlekkeloos Nederlands. “Later zal ik mezelf identificeren, maar voorlopig wil ik anoniem blijven.”

De man gaat verder. “Voordat we beginnen, wil ik in Nederland politiek asiel aanvragen. Binnen enkele uren verwacht ik dat de Bulgaarse regering Nederland zal vragen mij uit te leveren. Daar zit de leider van de bende achter, die ik jullie gisteren in handen heb gespeeld. Hij heeft veel invloed in Bulgarije. Tijdens mijn proces wordt de rechter omgekocht en krijg ik de doodstraf – als ik geluk heb.”

Peter frons zijn wenkbrauwen. “Je bent een informant? Ik neem aan dat je dat kunt bewijzen. Ik zal je asielaanvraag straks doorgeven aan de Immigratiedienst. Eerst moet je ons het complete verhaal vertellen. Als ik merk dat je liegt, zorg ik er voor dat je Nederland wordt uitgezet.” De man knikt kort en begint te vertellen.

20 DECEMBER 10:13

#### *Den Haag, Bulgaarse ambassade*

“Spreek ik met de ambassadeur?”

“Daar spreekt u mee. Waarmee – ”

“Luister goed. Ergens in Amsterdam wordt een voormalig lid van onze geheime dienst vastgehouden. Die persoon moet onmiddellijk terug naar Bulgarije, hij mag geen gevoelige informatie doorspelen naar de Nederlandse autoriteiten.”

“Duidelijk. En als Nederland die persoon niet wil uitleveren?”

“Voor die situatie sturen we iemand van ons mee. We weten binnen één uur waar onze landgenoot wordt vastgehouden. Zorg dat er dan een diplomaat klaar staat om hem op te halen.”

20 DECEMBER 10:14

#### *Geheime locatie in Amsterdam-Zuidoost*

Enkele jaren geleden is de man bij de bende gekomen toen de Bulgaarse geheime dienst werd afgeslankt. Met zijn universitaire it-kennis en zijn cybertools kon hij de toenmalige leider van de bende snel imponeren door in 30 minuten het emailaccount en de voicemailbox van een Amsterdamse officier van Justitie te kraken.

“We gingen naar Nederland omdat er veel computers met breedbandverbindingen in gebruik zijn, die bovendien bijna allemaal werken met dezelfde software. De meeste organisaties standaardiseren op de marktleidende software, omdat ze denken dat ze door schaalvergroting kosten kunnen besparen. Ze negeren daarbij de kosten van cyberincidenten. Veel computers met dezelfde software is gunstig voor ons, omdat we dan met één virus alle machines kunnen besmetten. We verdienen veel geld met het versturen van spam, computervirussen en met afpersing van organisaties en personen, bijvoorbeeld

met bedrijfsgeheimen of buitenechtelijke relaties. Zoals met die politicus vlak voor de verkiezingen van 2010, daar hebben we aardig aan verdiend. Zelfs als er geen gênante informatie op een computer staat, dan kunnen we altijd gevoelig materiaal uploaden en dreigen de politie te tippen. Meestal betalen ze grif”.

“De computers van mensen thuis lijken me gemakkelijk te hacken. Maar bedrijven hebben toch meestal een goede beveiliging?” vraagt Peter.

“Beveiliging wordt minder effectief door de enorme groei van cybercrime. Antiviruspakketten lopen steeds meer achter en detecteren nog maar maximaal 70% van de nieuwste virussen. Dat soort beveiligingsmaatregelen maakt het hooguit ietsje moeilijker om computers te besmetten. We testen nieuwe virussen uitgebreid om te voorkomen dat ze snel worden gedetecteerd, anders genereert zo’n virus voor ons geen inkomsten meer. In 2011 is in een Europees onderzoek vastgesteld dat bijna alle Nederlandse computers dat soort beveiligingsmaatregelen had, maar dat Nederland met 23% besmettingen toen nog middelmatig scoorde. Maar onze inkomsten verminderden doordat het gebruik van Open Standaarden in 2012 binnen Nederland een grote vlucht nam.”

“Open Stand – Wat heeft dat er nou mee te maken?” valt Peter hem geïrriteerd in de rede.

De man knipoogt naar Chris. “Hieruit blijkt dat jouw gebrek aan visie op it-gebied gecompenseerd moet worden ... door je collega?”

Chris glimlacht en Peter wordt rood in zijn gezicht: “Zegt de visionair die door de politie is neergeschoten en gearresteerd!”

“Dat heb ik zelf zo opgezet, maar dat vertel ik later. Laat ik het simpel uitleggen. Alle software bevat kwetsbaarheden die inbreken mogelijk maken. Waarom denk je dat er veel meer virussen in omloop zijn voor bijvoorbeeld het Windowsplatform en minder voor Linux?”

“Waarom Windows de meeste virussen heeft? Da’s makkelijk, dat komt natuurlijk door het grote marktaandeel. Maar ook al is Linux beter dan Windows, als Linux net zoveel marktaandeel krijgt als Windows, volgen de virussen vanzelf.”

“Met dat rookgordijn vliegen veel mensen uit de bocht” merkt de man op. “Het gaat namelijk helemaal niet over Windows versus Linux, of de Mac. Het gaat om keuzevrijheid. Of liever gezegd, het GEBREK aan keuzevrijheid.”

Peter kijkt hoopvol naar Chris, die kucht: “Vandaar die Open Standaarden?”

De man verzet zijn gewonde been en trekt een grimas. “Precies! Computergebruikers zullen pas veranderen van software, als ze zich niet druk meer hoeven te maken over uitwisseling van data en vertrouwen hebben in de alternatieve software. Hoe meer verschillende software wordt gebruikt, hoe meer het risico van cybercrime wordt gespreid. In Nederland gaf de overheid in 2012 het goede voorbeeld door zoveel mogelijk voor Open Standaarden te kiezen en op het gebruik daarvan actief te sturen. Bovendien zorgde de bezuinigingen ervoor dat de overheid waar mogelijk overschakelde naar gratis Open Source software. Leveranciers van betaalde software schreeuwden natuurlijk moord en brand, maar het viel politiek niet te verkopen veel ambtenaren te ontslaan, terwijl er miljoenen voor software wordt uitgegeven als gratis software ook voldoet. Na dit voorbeeld van de rijksoverheid volgden de vitale sectoren en het bedrijfsleven op enige afstand. Daardoor verminderde de software monocultuur in Nederland langzamerhand.”

Peter leunt achterover. “Net zei je dat er in Nederland op zoveel computers dezelfde software draait. De marktaandelen van software in Nederland zijn de afgelopen jaren nauwelijks veranderd. Moet ik geloven dat zoveel mensen in zo’n korte tijd allemaal van software zijn veranderd?”

“Met een wiskundig model voor de verspreiding van virussen kun je uitrekenen dat iets meer

softwarediversiteit de verspreiding van virussen al effectief verhindert. Als meer mensen migreren naar niet-marktleidende software dan er virusbesmettingen zijn, sterven volgens de theorie alle virusbesmettingen uit.”

“Ja, dat zou kunnen. En wat dan nog? Zelfs al veranderen sommige mensen van bijvoorbeeld Windows naar de Apple, dan kun je daar nog steeds virussen voor ontwikkelen?”

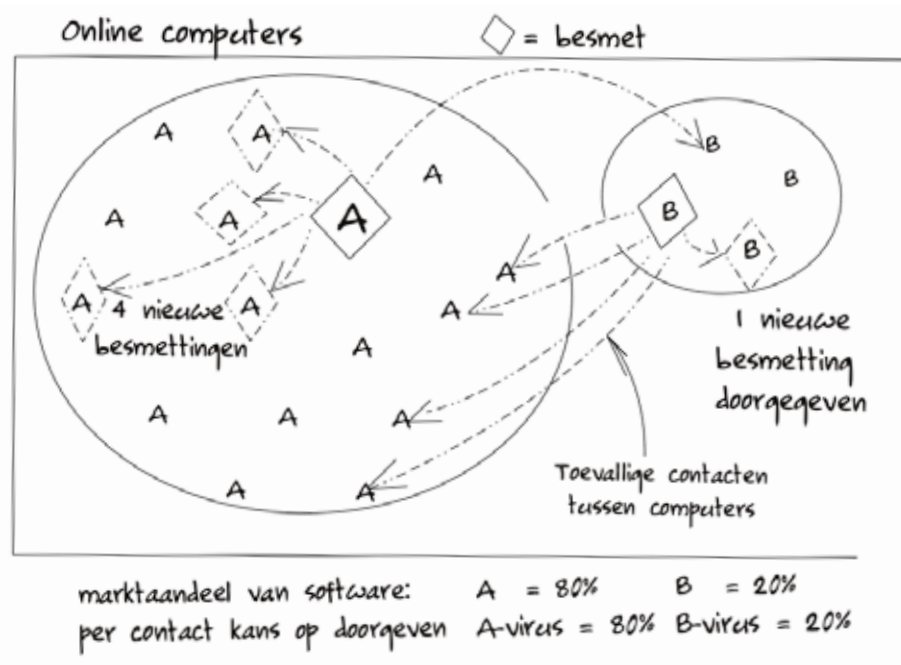
De man rolt zijn rolstoel dichterbij de tafel en zegt: “Dat kan wel, maar OF dat ook gebeurt is afhankelijk van het marktaandeel van die software. Ik kan het voor je uittekenen.”

Peter haalt een plastic pen uit zijn colbert en schuift die met een vel papier over de tafel naar de man. De man begint te tekenen en legt tegelijkertijd uit.

“Kijk, het kopen of ontwikkelen van een virus kost ongeveer evenveel geld, welk platform je ook kiest. Dat geld kan je terugverdienen als het virus niet voortijdig uitsterft. Hoe groter het marktaandeel is van het platform dat het virus aanvalt, hoe kleiner die kans is.”

“De computers binnen dezelfde cirkel gebruiken dezelfde software. Andere cirkel betekent andere software. Stel dat software A in de grote cirkel een marktaandeel heeft van 80% en software B in de kleine cirkel 20% marktaandeel.”

De man wijst op het papier. “In principe kan een besmette A-computer geen B-computers besmetten en vice versa. Alleen als een besmette computer toevallig contact maakt met andere computers in dezelfde cirkel, kan het virus zich vermenigvuldigen. Daarnaast heeft elke besmette pc een bepaalde kans om zijn besmetting kwijt te raken, bijvoorbeeld met antivirussoftware. Als je aanneemt dat bij een contact tussen A-computers de kans op besmetting en ontsmetting even groot is als voor B-computers, dan – ”



20 DECEMBER 10:45

### ***Amsterdam, Beurs van Berlage***

De woordvoerder van het Korps Nationale Politie opent de persconferentie en geeft aan dat er eerst een korte verklaring zal volgen over het oprollen van de bende die bekend staat als Cash & Curry. Daarna is er ruimte voor vragen.

Gisterochtend vroeg is de bende ingerekend, na een gecombineerde actie van het KNP en de Politie Regio Amsterdam. Deze bende hield zich sinds 2011 in Nederland bezig met het verspreiden van computervirussen en het versturen van spam. Daarnaast verkochten ze gevoelige informatie van de computers die ze met virussen hadden besmet en werden mensen en bedrijven daarmee afgeperst. In een bijna twee jaar durend politieonderzoek zijn diverse tips gecombineerd met digitale recherche, wat uiteindelijk tot de arrestatie van gisteren heeft geleid. Voorzover bekend zijn alle vijf de bendeleden ingerekend, die voornamelijk van Oost Europese afkomst zijn. Bij de arrestatie van de bende zijn enkele pc's, verschillende wapens met munitie en ca. 3,3 miljoen Euro aan contant geld in beslag genomen.

20 DECEMBER 11:03

### ***Geheime locatie in Amsterdam-Zuidoost***

Nadat ze de uitleg een poosje nadenkend had gevolgd, brak Chris in. "Ik snap het! Van elke 5 contacten tussen computers zijn er 4 met 'A' en maar één met 'B'. Omdat de kans op ontmetting voor 'A' en 'B' even groot is, maar er veel minder besmettingen voor 'B' worden doorgegeven, zal het B-virus dus veel sneller uitsterven. Omgekeerd is de kans veel groter dat een 'A' besmetting wordt doorgegeven."

De man kijkt Chris goedkeurend aan. "Juist. Het maximale aantal besmettingen is een evenwicht tussen de kansen voor besmetting en ontmetting. Daarom maximaliseert een monocultuur het risico van cybercrime. Als het merendeel van de mensen marktleidende software gebruikt, is de kans dat je een virus oppikt maximaal. Want de kans is groot dat deze besmetting vervolgens kan worden doorgegeven aan alle computers met dezelfde software. Dus kans maal impact is maximaal, waardoor een samenleving kwetsbaar wordt."

Peter merkt op: "Dat inzicht bestaat in de landbouw al veel langer. Percelen met hetzelfde gewas mogen niet te groot zijn en niet met elkaar verbonden zijn om ziektes en plagen tegen te gaan. Maar volgens mij is in Nederland de schade door cybercrime van 2012 tot 2016 niet gedaald."

De man schudt zijn hoofd. "Als je de Nederlandse cijfers over de groei en de omvang van cybercrime vergelijkt met de rest van Europa, dan zie je dat veel andere landen jaloers zijn op de Nederlandse situatie. Bijna overal groeit de schade door cybercrime veel sneller."

De man vervolgt: "Doordat in Nederland het rendement van virussen relatief minder werd, gingen we ons steeds meer richten op Engelstalige landen. Maar we kregen steeds meer concurrentie van andere cyberbendes. Ongeveer een jaar geleden was er een bende die onze gehackte computers probeerde over te nemen. Ze bleken zich ook bezig te houden met mensenhandel en het verspreiden van porno ... ook van jonge kinderen."

"Hoeveel ellende een dergelijke uitbuiting veroorzaakt, heb ik van dichtbij gezien." Met een donkere blik in zijn ogen wrijft de man langzaam in zijn handen. "Misschien loop ik er nog eens

eentje tegen het lijf ... Ik heb de computers van die bende gekraakt en kwam zo achter hun locatie en alle wachtwoorden van hun computers. Daarna heb ik die per brief doorgegeven aan de politie.” Peter herinnerde zich dat deze tip in het dossier zat. Op basis van deze tip had zijn team vorig jaar verschillende computers in beslag genomen en meegenomen voor onderzoek. Met een geheime, Europees gecoördineerde actie waren veel criminelen en ‘klanten’ gearresteerd, waarvan een groot aantal kon worden vervolgd met het bewijsmateriaal op deze computers.

“Om meer inkomsten te genereren wilde onze bendeleider daarna de mensenhandel van deze bende overnemen. Afscheid nemen van de bende bleek voor mij geen optie. Toen heb ik besloten de bende in handen van Justitie te geven. Sinds ‘n jaar heb ik de politie e-mails gestuurd met daarin verborgen boodschappen. In mijn laatste boodschap gaf ik aan dat alle benedeleden gisteren in de Van Woustraat verbleven, zodat jullie iedereen konden arresteren.”

Peter wist dat de politie sinds een jaar spottende e-mails van een niet-bestaand afzenderadres ontving die waren ‘ondertekend’ met steeds een andere afbeelding van een currygerecht. Net begonnen aan haar stage bij het Nationaal Cyber Security Centrum, had Chris na drie zulke berichten de verborgen boodschappen in die afbeeldingen gevonden. De boodschappen bevatten bewijzen over de criminele activiteiten van de bende, waarbij een aantal transporten van mensenhandelaren kon worden onderschept. Het verhaal van de man zou kunnen kloppen, maar zijn verhaal vormt nog geen bewijs. Zijn medewerking is echter essentieel om het hele verhaal boven water te krijgen.

20 DECEMBER 11:09

### ***Amsterdam, Beurs van Berlage***

Na de verklaring van de politie is de beurt nu aan de verzamelde pers. De eerste vraag: “De bende was al sinds 2009 operationeel in Nederland en de aanwijzing die leidde tot aanhouding van de bende was gevonden in een email van twee weken terug. Waarom duurde het zo lang voordat de bende kon worden opgerold?”

De woordvoerder geeft aan dat het KNP jaren nodig had om de bende op te sporen en de zaak qua bewijsvoering sluitend te krijgen, omdat de bende met professionele beveiligingskennis hun sporen wiste. Zo werd communicatie altijd gecijferd en werden de gehackte computers bestuurd via snel wisselende servers in het buitenland. Pas na diverse tips het afgelopen jaar van een infiltrant is de zaak in een stroomversnelling geraakt.

De volgende vraag vanuit de zaal: “Had de infiltrant de boodschappen ook ondertekend?” Het antwoord: “Ja, met de naam Nikolay, wat zo goed als zeker een schuilnaam is.”

GELIJKTIJDIG

### ***Geheime locatie in Amsterdam Zuid-Oost***

“Waarom wilde je tijdens de arrestatie je wapen niet neerleggen?” vroeg Chris.

“Drie maanden geleden betrapte de bendeleider mij toen ik zo’n email naar de politie stuurde. Hij wilde dat ik daarmee stopte. Met jullie inval zag de bendeleider zijn eerdere wantrouwen tegen mij in één klap bevestigd. Omdat hij gewapend was, moest ik hem onder schot houden totdat hij zijn pistool had losgelaten. Hij had me anders neergeschoten.”

Peter doet zijn armen over elkaar. “Ik heb nog geen snipper bewijs gezien dat jij de rol van infiltrant hebt ingevuld. Als je inderdaad infiltrant bent, leidt dat mogelijk tot strafvermindering en misschien wel tot politiek asiel. Zonder dat bewijs wordt je veroordeeld als lid van een criminele organisatie. Wat kun je ons nog meer vertellen?”

Op dat moment worden de persoonlijke bezittingen van de man de verhooruimte ingebracht: een portefeuille met een afgescheurd stuk papier erin, waarop ‘Nikolay’ staat geschreven. Chris pakt fronsend het papier op en legt dat naast het bewijsstuk uit de zaak van een jaar geleden waarop de wachtwoorden van de computers waren geschreven. De scheurranden blijken perfect aan te sluiten. Daarnaast is het handschrift op het bewijsstuk en de toelichting van de man identiek. Chris neemt Peter apart en zegt zachtjes: “Hij moet Nikolay zijn.”

Veel tijd om hierover na te denken krijgen Peter en Chris niet. De gsm van Peter gaat over. Er is een team van de Bulgaarse ambassade gearriveerd dat de arrestant direct wil meenemen. Met een wrang gevoel loopt Peter naar de ingang en ziet dat het team bestaat uit ‘n dunne man gekleed als een diplomaat en één breedgeschouderde man met gemillimeterd haar en indringende ogen.

“De verdachte wordt momenteel nog verhoord. U kunt deze persoon dus nog niet meekrijgen,” probeert Peter. De diplomaat glimlacht flauwtjes en geeft hem een briefje. “Belt u dat nummer alstublieft. We hebben haast.”

Peter belt en heeft daarop vrijwel direct de directeur-generaal Internationale Samenwerking aan de lijn. Hij geeft Peter opdracht de arrestant onmiddellijk over te dragen aan het team voor uitlevering aan Bulgarije, vanwege misdaden daar gepleegd. Peter werpt tegen dat de arrestant zojuist politiek asiel heeft aangevraagd. Bovendien lijkt de man kennis te bezitten die zeer waardevol is in het politie-onderzoek. Na drie minuten heen en weer gepraat wordt het gesprek geforceerd beëindigd, terwijl het team steeds ongeduldiger wordt. “De uitlevering is al afgestemd met uw baas en het OM. Als u niet meewerkt, laat ik de zaak binnen een kwartier overdragen aan iemand anders.”

Als Peter voor het overdrachtsdocument wil tekenen, merkt hij dat hij zijn pen mist. Hij ondertekent met een geleende pen en loopt met het team van de diplomatieke dienst terug naar de verhooruimte. Als ze de deur openen, hangt Chris happend naar adem met handboeien vastgeketend aan de verwarmingsbuis. Ze fluistert hees: “... slag tegen mijn keel ... Nikolay ... handboeien los ...” Op tafel ligt de pen waar de metalen clip van is afgebroken.

Peter ziet uit zijn ooghoeken op zijn stoel de volgende boodschap, geschreven op de achterkant van het papier.

*Beste Peter,*

*aan de informatie op je werk pc en je thuis pc zag ik dat je te vertrouwen bent. Met de Taj Mahal actie en wat druk achter de schermen heb ik jou als leider van het onderzoek laten benoemen, zodat jij de bende kon arresteren.*

*Zoals je begrijpt kies ik voor vrijheid in plaats van uitlevering naar mijn moederland. Misschien komen we elkaar nog eens tegen?*

*Hartelijke groet,*

*Nikolay*

Terwijl hij de boodschap camoufleert door erop te gaan zitten, tuimelen allerlei gedachten door Peter's hoofd. Was Nikolay indertijd wel ontslagen bij de Bulgaarse Geheime Dienst? Heeft hij zich misschien schuldig gemaakt aan spionage in Nederland? En ...  
Door het open raam waait sneeuw de kamer in, de voetstappen buiten al bijna gewist.

**Henk-Jan van der Molen** is als docent verbonden aan de Hogeschool Wageningen. Hij doceert binnen de opleiding Bedrijfskundige Informatica onder meer Business Intelligence, Informatiebeveiliging en Verandermanagement. Ook vanuit zijn praktijkervaringen heeft hij artikelen gepubliceerd in o.a. Computable.nl, het PvIB blad Informatiebeveiliging, het Amerikaanse ISACA Journal en NRC Handelsblad.

