Open einde

Henk-Jan van der Molen Erik Kriek

Henk-Jan van der Molen is naast projectmanager Security bij I-Interim Rijk ook freelance docent bij de Security Academy. In een kort verhaal beschrijft hij waarom het zo belangrijk is open standaarden te gebruiken. Alles aan deze tekst is fictief, behalve de feiten over open standaarden.

Buiten sneeuwt het. Binnen verlicht een kale gloeilamp de kamer, de verwarming tikt. Commissaris Peter Both wacht op de laatste verdachte. De arrestatie gisteren was de kroon op het lange onderzoek van het Team High Tech Crime van politie.

‘Peter!’ Hij schrikt op. Christa de Vries, digitaal rechercheur bij het Nationaal Cyber Security Centrum knipoogt.

‘Korte nacht? Wil je zijn dossier?’ Peter geeuwt: ‘Straks. Tot dusver heeft niemand iets losgelaten. Deze arrestant vroeg speciaal naar mij als onderzoeksleider. Ik wil eerst horen wat hij te zeggen heeft.’

De arrestant wordt geboeid binnengereden in een rolstoel – bij de inval gisteren schampte een politiekogel zijn been.

Peter start de recorder: ‘Who are you?’ De man antwoordt in vlekkeloos Nederlands:

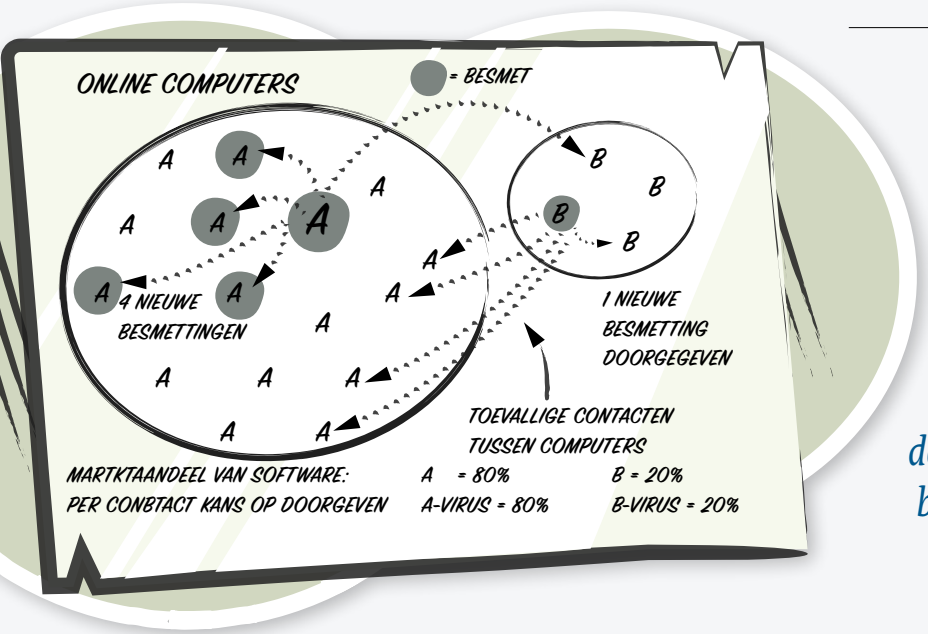
‘Later. Voorlopig wil ik anoniem blijven … Voordat we beginnen, ik wil in Nederland politiek asiel aanvragen. Vandaag zal de Bulgaarse regering vragen om mijn uitlevering. De bende die ik jullie gisteren in handen heb gegeven, heeft veel invloed in Bulgarije. De rechter wordt omgekocht en ik krijg de zwaarst denkbare straf.’

Peter fronst: ‘Jij, een informant? Ik zal je asielaanvraag doorgeven aan de Immigratiedienst. Maar vertel eerst je verhaal. En probeer niet te liegen.’ De man knikt kort en begint te vertellen.

Enkele jaren geleden kwam de man bij de bende, nadat de Bulgaarse geheime dienst werd afgeslankt. Vanwege de werkrelaties en infiltratie tussen de beide partijen voor hem geen vreemde stap.

‘We kozen Nederland als werkterrein, omdat veel organisaties standaardiseren op marktleidende software. Ze denken dat ze zo kosten besparen. Wij kunnen met één virus eenvoudig vrijwel alle computers besmetten. We verdienden veel geld met afpersing van organisaties met bedrijfsgeheimen. Of personen, zoals een politicus met zijn maîtresse, vlak voor de verkiezingen. Ook plaatsten we gevoelig materiaal op een computer en dreigden de politie te tippen, waarna er grif werd betaald.’

‘Privécomputers zijn makkelijk te hacken. Maar bedrijven hebben toch meestal een goede beveiliging?’, vraagt Peter.



Peter schuift een pen en een vel papier over de tafel en de man begint te schetsen

‘Beveiliging kan de groei van cybercrime niet bijhouden. Antiviruspakketten lopen steeds meer achter.
We testen nieuwe virussen om te voorkomen dat ze snel worden gedetecteerd. In 2012 leek het nog even of Nederland massaal open standaarden zou gaan gebruiken, maar …’
‘Wat heeft dát er nou mee te maken?’, onderbreekt Peter. ‘Laat ik het simpel uitleggen', zegt de man. ‘Alle software bevat kwetsbaarheden die inbreken mogelijk maakt. Maar voor Windows zijn veel meer virussen dan voor Linux.’
‘Dat snap ik', zegt Peter. 'Omdat Windows een groter marktaandeel heeft. Als Linux groeit, volgen de virussen vanzelf.’
‘Maar het gáát niet over Windows versus Linux’, merkt de man op. ‘Het gaat om keuzevrijheid. Of beter gezegd, het gebrék aan keuzevrijheid door de afhankelijkheid van bepaalde software te versterken.’

Peter kijkt met een blik vol vraagtekens naar Christa. Die zegt: ‘Vandaar open standaarden?’
De man verzet zijn gewonde been en trekt een grimas.
‘Precies! Computergebruikers veranderen pas van software als de alternatieve software correct werkt met dezelfde bestanden. Hoe meer verschillende software wordt gebruikt, hoe beter het risico van cybercrime wordt gespreid. De Nederlandse overheid wilde in 2012 met open standaarden de afhankelijkheid van bepaalde software te verminderen. Maar leveranciers van betaalde software in de VS startten toen in Europa een lobby voor hun producten. En met succes: Europa – en daarmee ook Nederland – is door gebrek aan visie en durf sterk afhankelijk gebleven van die software uit de VS. Het passief ondersteunen van open standaarden alleen is dus niet voldoende. Dan blijven computergebruikers bij de software die ze al jaren gebruiken. En zo konden wij heel eenvoudig veel computers blijven besmetten. Onze inkomsten bleven groeien.’

Peter leunt achterover. ‘Met andere software wordt de beveiliging toch niet beter?’
‘Met andere software niet nee, maar wel met meer kéuze voor software. Met een wiskundig model kun je uitrekenen dat iets meer softwarediversiteit de verspreiding van virussen al remt. Theoretisch kunnen alle virusbesmettingen zelfs uitsterven als genoeg mensen overstappen naar alternatieve software.’
‘Dat geloof ik niet. Zelfs al vervangen sommige mensen Windows door Linux, dan kun je daar toch nog steeds virussen voor ontwikkelen?’
De man trekt zijn rolstoel dichter naar de tafel en zegt: ‘Ik zal het voor je uittekenen.’
Peter schuift een pen en een vel papier over de tafel en de man begint te schetsen.

‘Het ontwikkelen van een virus kost ongeveer evenveel geld, welk platform je ook kiest. Dat geld verdien je terug als je virus niet voortijdig uitsterft. Hoe groter het marktaandeel is van de software die het virus aanvalt, hoe kleiner die kans is. De computers binnen dezelfde cirkel gebruiken dezelfde software. Stel dat software A in de grote cirkel een marktaandeel heeft van 80% en software B in de kleine cirkel 20%.’
De man wijst op het papier. ‘Een besmette A-computer kan geen B-computers besmetten en omgekeerd. Alleen als een besmette computer contact maakt met andere computers met dezelfde software, 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 onderling contact tussen A-computers de kans op besmetting en ontsmetting even groot is als voor B-computers, dan …’
Opeens roept Christa: ‘Ik snap het! Van elke vijf contacten tussen computers zijn er vier met ‘A’ en maar één met ‘B’. Omdat de kans op ontsmetting 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 Christa goedkeurend aan. ‘Juist. Cybercriminelen maken dus de meeste virussen voor marktleidende software. In een monocultuur is namelijk zowel de kans op een cyberaanval als de impact daarvan maximaal. Onze verdiensten zijn dan ook optimaal.’
Peter doet zijn armen over elkaar. ‘Als je inderdaad infiltrant bent, krijg je mogelijk strafvermindering en misschien zelfs politiek asiel. Zonder bewijs word je veroordeeld als lid van een criminele organisatie.
En ik heb nog geen snipper bewijs gezien …’
Voordat de man hierop kan antwoorden, gaat Peters mobiel over. Het is de directeur-generaal Internationale Samenwerking die hem opdracht geeft de arrestant onmiddellijk over te dragen. Bulgarije wil hem berechten voor zijn misdaden. Terwijl Peter de gang in loopt, werpt hij tegen dat de arrestant politiek asiel heeft aangevraagd. Bovendien heeft de man waardevolle kennis voor dit onderzoek. Na drie minuten eindigt het gesprek geforceerd: ‘De uitlevering is al afgestemd met uw baas. Twee mannen komen hem zo halen. Als u niet meewerkt, dan laat ik uw onderzoek binnen een kwartier overdragen aan iemand anders.’

Peter loopt terug richting de verhoorruimte. Als hij de deur opent, hangt Christa met handboeien vast aan de verwarmingsbuis. Met piepende adem zegt ze: ‘Onze arrestant … handboeien los … slag tegen mijn keel …’

De gedachten tuimelen door Peters hoofd. Was deze man echt informant? Was hij indertijd wel ontslagen bij de Bulgaarse geheime dienst? Spioneerde hij misschien in Nederland? En …
Door het open raam waait sneeuw de kamer in, de voetstappen buiten zijn al bijna uitgewist.