

Aanpak cybercrime gebaat bij innovatiekracht open source software

Met de komst en de groei van het internet, is ook de rol van de digitale opsporing geïntroduceerd. En daarmee de software die ermee gemoeid is. In Nijmegen, in het hoofdbureau van de **Politie Gelderland-Zuid, wordt sinds een aantal jaar gewerkt aan het ontwikkelen van (onderzoek- en opsporings-) toepassingen, waarbij in 2006 een bewuste keus is gemaakt voor open standaarden en open source software. Vanwege de kosten, maar vooral vanwege het innovatieve karakter van open source.**

Een van de doelen van het huidige (demissionaire) kabinet is dat de criminaliteit in Nederland in 2010 met 25 procent gedaald moet zijn ten opzichte van 2002. Twee van de afspraken daarbij zijn dat de opsporing versterkt wordt en dat georganiseerde misdaad, financieel economische criminaliteit en cybercrime steviger aangepakt worden. Zo valt te lezen op de website van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties ([http://www.bzkr.nl](#)). Met name cybercrime (criminaliteit op of met behulp van internet) is de laatste jaren een hot item geworden. De groei ervan heeft er onder meer toe geleid dat vandaag de dag een flink deel van de tijd en menskracht binnen de verschillende Nederlandse politiekorpsen ingeruimd wordt voor het opsporen van cybercrime, en het ontwikkelen van toepassingen die daar toe kunnen bijdragen. Een van de mensen die zich dagelijks bezighoudt met het ontwikkelen van (onderzoek- en opsporings-)toepassingen, is Peter de Beijer, projectleider Interregionaal Project Internet Recherche & Project Web Observatie bij de Politie Regio Gelderland-Zuid. De Beijer kwam in 1985 in dienst van (toen nog) de gemeentepolitie van Nijmegen, liep een aantal jaren in het 'blauw', maar werd tegelijkertijd gegrepen door zijn tweede grote passie: ICT. Hij besloot op HBO- en universitair niveau een aantal ICT-studies te volgen, en raakte vervolgens begin jaren '90 toevalligerwijs betrokken bij een van de door het ministerie van BZK opgezette pilots over computercriminaliteit. "Destijds was ik vanuit de gemeentepolitie Nijmegen eigenlijk de enige die een 'blauwe' achtergrond combineerde met een ICT-achtergrond, en dat was reden om mij bij het project te betrekken. Dat is zo goed bevallen, dat ik sinds die tijd niet meer weggegaan ben uit dit onderdeel van het politievak."

Open source software

Waar de afdeling van De Beijer zich in eerste instantie onder meer bezighield met huiszoeken (zoals het veilig stellen van pc's en het verzamelen van bewijsmateriaal), daar is het inmiddels doorgesloegen naar een soort van tweedelijns ondersteuning. "Deze afdeling (7,5 FTE in totaal en 2,5 FTE voor het project Internet Recherche & Onderzoek Netwerk, FdJ) bestaat vandaag de dag hoofdzakelijk uit mensen met HBO ICT-kennis die zich vrijwel volledig richten op ontwikkeling. Ons werkgebied zijn daarbij voornamelijk de zes oostelijke regio's. Door de verschuiving van werkzaamheden worden huiszoeken en dergelijke tegenwoordig door de bureaus digitale recherche opgepakt", zo zegt De Beijer, die al in een relatief vroeg stadium in aanraking kwam met open standaarden en open source software.

"Het zal ergens in 2004 zijn geweest dat de recherche-afdeling bij ons kwam om te praten over hun veranderende rol binnen de politie. Debet daaraan was met name de forse groei van het internet. Zij vonden dat, vanuit hun opsporing- en onderzoeksgedachte, het internet een belangrijke rol zou moeten spelen in hun werkzaamheden, ook al omdat ze zagen dat hun klandizie naar het internet aan het verschuiven was. Zelf hadden ze echter geen idee of ze tot dan toe goed bezig waren, en bij de ICT-afdeling kregen ze onvoldoende gehoor. Onze eerste gedachte was: 'dan maken we een leuk stukje techniek, en dan zijn ze wel tevreden'. Dat had technisch gezien makkelijk gekund, en bovendien waren we dan snel klaar geweest. Gelukkig hebben we die stap niet gemaakt. In plaats daarvan hebben we een stapje teruggedaan en eerst eens goed gekeken hoe we het eigenlijk zouden willen aanpakken. Daar is uit voortgekomen dat ons een eigen netwerk voor ogen stond waarin we een interne ISP-achtige

(intranet) omgeving wilden vormen voor onderzoek en opsporing. We kwamen al snel tot de conclusie dat dát niet kon met de toenmalige Windows-omgeving. Dan hadden we enerzijds ons budget flink moeten verhogen, en anderzijds zouden we in de toekomst onherroepelijk vastgelopen zijn. Ook omdat we destijds al redelijk precies wisten welke richting we uit wilden. We hebben de keus gemaakt, en dat had betrekking op alles wat we vanaf die tijd nog zouden ontwikkelen, dat dát alleen maar kon als we de overstap zouden maken naar open source software.”

Innovatie

In de keus van De Beijer en zijn projectteam voor open source software (Linux/Ubuntu specifiek, FdJ), heeft kostenbesparing zeker een rol gespeeld. Toch was dat niet hét argument om de overstap naar ‘open’ te maken. De Beijer resoluut: “Dat was innovatie. Met name de innovatiekracht van open source software is enorm en ook nog eens zodanig zonder dat we met Jan en alleman commercieel in zee hadden moeten gaan. Of grote bedragen hadden moeten ophoesten om bepaalde functionaliteit te krijgen. Wat verder een rol heeft gespeeld in de beslissing voor open source software, was de mogelijkheid om makkelijker met andere partijen samen te werken. Binnen de sector (Openbare Orde en Veiligheid) doen we dat graag en ook steeds vaker (bijvoorbeeld met de 25 politieregio’s, het Korps Landelijke Politie Diensten, Openbaar Ministerie, de Politie Academie, bijzondere opsporingsdiensten en een aantal toezichthouders, FdJ)”, aldus De Beijer, die met name de ontwikkeling bij het Amerikaanse bedrijf Google als ‘zeer interessant en inspirerend’ bestempelt. “Ik ben met name gecharmeerd van de manier waarop zij omgaan met de ontwikkeling van het internet. Met hen ben ik ervan overtuigd dat op internet hét de komende jaren gaat gebeuren. Het internet gaat voor een groot deel bepalen wat wij doen, en gaat ook bepalen hoe wij met informatie om zullen gaan. Als politie-organisatie zullen wij daarin een rol moeten spelen. Het mooie is dat we daarbij niet alles zelf hoeven te ontdekken of te bedenken, maar je moet wel zorgen dat je snel koppelingen met andere partijen of ontwikkelingen kunt maken.”

Tijdens het gesprek benadrukt De Beijer meerdere malen dat de tactiek in het gehele proces leidend is geweest. “Wat we in de praktijk zien, wordt vertaald naar de techniek toe. Niet andersom. Ik was daarbij in de gelukkige omstandigheid dat ik ruim 14 jaar ervaring in mijn bagage had zitten met betrekking tot digitale opsporing. Dat gaf mij, en daarmee ook anderen binnen ons team, goed inzicht in waar behoefte aan was.” Nadat in eerste instantie die behoefte was geïnventariseerd, werd vervolgens ongeveer een jaar uitgetrokken om de basisinfrastructuur op te zetten. “We zijn daarbij begonnen met niets, en hebben alles stap voor stap opgebouwd”, zo laat Peter de Beijer weten, die op dat punt wordt aangevuld door Wim Michels, Senior Adviseur Informatiemanagement bij de Politie Regio Gelderland-Zuid, en waarnemend hoofd. “De eerste resultaten waren er toen aan het eind van 2006 circa 25 werkplekken waren ingericht voor een kleine 70 gebruikers”, aldus Michels. “Dankzij voorlichting en de nodige mond-tot-mondreclame is dat uitgegroeid tot een systeem dat vandaag de dag 330 werkplekken heeft, dwars door het land, waaraan circa 1400 gebruikers hangen. Opvallend is dat het basisconcept in al die jaren eigenlijk hetzelfde is gebleven, net als het aantal mensen dat het project bestiert. Dat ondanks de forse groei van het aantal gebruikers en de verschillende deelprojecten met wisselende externe partijen. Met mijn ‘traditionele’ IT-ervaring vind ik met name dat laatste toch wel erg verrassend.”

Transparantie

Innovatie, samenwerken, kostenbesparing: het zijn een paar van de beweegredenen die voor Peter de Beijer en zijn team belangrijk zijn geweest bij de keus voor ‘open’. Nog niet genoemd is het ‘thema’ transparantie. “Onze gebruikers houden zich specifiek bezig met onderzoeken en opsporen op internet. Een deel van die informatie wordt gebruikt, of kan gebruikt worden, in straf- en rechtszaken. Dat betekent dat wel transparant moet zijn waar die informatie vandaan komt. Om die reden wordt al het surfverkeer van onze gebruikers vastgelegd, gelogd

zagezegd. Die vastlegging gebeurt 'onder water', zodat de gebruiker de informatie wel kan bekijken, maar er verder niet bij kan. Een en ander hebben we ingebouwd omdat zo'n systeem geschikt moet zijn voor bewijsvoering en ook nog eens toetsbaar moet zijn. Bijvoorbeeld door het Nederlands Forensisch Instituut. Met deze opzet, die onder meer uitgebreid is doorgesproken met het Openbaar Ministerie, willen we voorkomen dat de niet-technische eindgebruiker verantwoordelijk wordt voor de techniek waarmee hij of zij die informatie vindt. Het komt er op neer dat er een knip is gemaakt in de verantwoording. Als projectteam zijn wij verantwoordelijk voor de infrastructuur, de techniek en de ontwikkeling, terwijl de eindgebruiker alleen verantwoordelijk is voor wat hij of zij ziet. Belangrijk in het kader van transparantie is ook dat een rechter bijvoorbeeld kan vragen naar de gang van het onderzoek- en opsporingsproces. Tot nu toe is het nog niet voorgekomen dat een rechter daar om heeft gevraagd, maar de mogelijkheid is er wel. En die mogelijkheid is er dankzij de aanwezigheid van alleen maar open source componenten, van begin tot eind", aldus De Beijer.

Open framework

Peter de Beijer is ook projectleider van een nieuw ontwikkeltraject (een afgeleide van het originele project uit 2006), waar met financiële steun van het ministerie van BZK en een groot aantal partijen gewerkt wordt aan een open (source) framework. "Dat is een project dat we samen doen met onder meer een aantal Nederlandse universiteiten en de Europese Unie, en als doel heeft om meer structuur aan te brengen in het onderzoek- en opsporingstraject op internet. Nu kan het voorkomen dat 26 collega's van evenzovele organisaties uit de OOV-sector op hetzelfde tijdstip naar dezelfde informatie zitten te kijken. We werken nu aan een systeem dat, voordat er een onderzoeksopdracht wordt uitgevoerd, eerst meldt of een dergelijke opdracht al niet is gedaan door een collega. Dat moet uiteindelijk een grote verspilling van tijd en menskracht tegengaan. Daarnaast willen we met behulp van dit open framework de gehele filosofie van het handmatig onderzoek omdraaien. Het is de bedoeling dat je straks een sms'je, mailtje of pop-up op je smartphone krijgt, op het moment er op internet activiteit is omtrent de onderwerpen waarvoor jij belangstelling hebt. Dat is vele malen handiger en sneller dan de huidige manier van digitaal onderzoek. Gelukkig beseffen ook steeds meer partijen dat. Zo merken wij dat de belangstelling om aan te haken met de week toeneemt. Onder meer de Universiteit van Amsterdam (UvA) en de Radboud Universiteit in Nijmegen zijn aangehaakt. Beide onderwijsinstellingen zijn bezig deelcomponenten voor het open framework te ontwikkelen, en met de Radboud zijn wij in gesprek om een aantal deelprojecten weg te zetten als stageopdracht bij Master-studenten. Dat is het mooie aan open source software: het maakt het makkelijk om met andere partijen samen te werken. Ik moet eerlijk zeggen dat binnen een toch wel hiërarchische organisatie als de politie dat nog steeds wel als enigszins vreemd wordt ervaren. Eigenlijk zijn wij dan ook een buitenbeentje. Zolang dat zo is, zitten we op de goede weg", zo lacht De Beijer."

Leermomenten

Gevraagd naar de leermomenten van de afgelopen jaren, blijft het aan de kant van Peter de Beijer een paar seconden stil. "Eigenlijk", zo vervolgt hij, "zijn er geen ontwikkelingen geweest waarvan we achteraf hebben gedacht: dat moeten we niet meer doen. Het is wel zo dat je relatief vaak 'producten' weggooit die niet interessant zijn of niet werken. We lanceren constant nieuwe dingen waarvan we denken: dat kunnen we wel even tussendoor prutsen, of daar hebben we wel even tijd voor. Dat is het voordeel van het werken met open source software. Bovendien is er het voordeel dat we alle software in eigen huis ontwikkelen. Dat zelf ontwikkelen is zeker bepalend, en dat willen we ook volhouden. En als we het laten ontwikkelen door een externe partij, bijvoorbeeld door de universitaire wereld, dan is er de afspraak dat de codes voor ons zijn. Ons streven is dat straks de codes binnen de overheid gedeeld kunnen worden. Dat betekent dat je óf een aansluiting neemt op ons netwerk, óf de

code krijgt en doe er dan vooral je eigen ding mee. In ieder geval wil ik die kosten niet twee keer voorbij zien komen. Ook niet als het gaat om veiligheid.”

Tot op de dag van vandaag is er niemand geweest die tegen Peter de Beijer of Wim Michels heeft gezegd dat hij een slechte keus heeft gemaakt om voor open standaarden en open source software te kiezen. “Ook niet als gekeken wordt naar de veiligheid van het systeem. Het betekent wel dat wij continue kijken naar wat er op het internet gebeurt, en naar de community’s die rondom de verschillende pakketten zijn gevormd. Als de community begint te twijfelen, twijfelen wij mee. En tegen iedereen die zich afvraagt of deze keus wel veilig is, zeggen wij: kom maar kijken, dan kun je zelf zien wat er onder de motorkap gebeurt...”

Samenwerkingspartijen die gebruikmaken van het IRN (Internet Recherche & Onderzoek Netwerk):

- 25 politie regio’s (waaronder grote regio’s als KLPD, Rotterdam-Rijnmond, Amsterdam-Amstelland, Haaglanden en Utrecht);
- 7 bijzondere opsporingsdiensten;
- toezichthouders van een aantal ministeries.

Binnen de IRN-projecten wordt onder meer gebruikgemaakt van de volgende software:

- Linux (Ubuntu);
- BSD;
- Joomla!;
- WordPress MU;
- OpenOffice.org;
- Apache.

Tekst: Frits de Jong – 2010

Geschreven voor Nederland Open in Verbinding (www.noiv.nl)