

COMPUTABLE

SECURITY / ACHTERGROND

09-09-2009 07:48 | Door Jolein de Rooij Gerelateerde bedrijven: Com-Connect

Rechercheur leert gestructureerd speuren

In de cursus Digitaal Rechercheren, die het Limburgse Com-Connect geeft, leren opsporingsmedewerkers tools en websites kennen waarmee ze hun speurwerk sneller kunnen doen. Daarnaast wordt ze bewustzijn bijgebracht van de gevaren van het internet. De cursusleider: 'Als je op een site komt waar herkenning mogelijk is, wil ik dat je dat anoniem doet.' Computable nam een kijkje.



'Dat moest anoniem, hè?' De cursist krijgt een tikje op zijn schouder van de jonge cursusassistent. 'Daarom surfte ik terug', zegt de dertiger. 'Dan is het al te laat', houdt de cursusassistent vol. 'Je wilt toch doorklikken, hè', zegt de dertiger. Cursusleider Wilfred van Roij, een slanke veertiger in spijkerbroek komt aansnellen en zegt: 'Ik betrap mezelf er ook nog vaak op. Het is toch een stukje adrenaline. Je denkt: ik héb hem.' Van Roij kan het weten. Twee jaar geleden was hij nog digitaal rechercheur bij de politie in Noord-Limburg.

Nu geeft hij les in Digitaal Rechercheren bij Com-Connect, een informatiebeveiligingsbedrijf onder de rook van Venlo. De vijf cursisten zijn casual gekleed, maar hebben één ding gemeen: de alerte blik in hun ogen. Het zijn allemaal onderzoeks-medewerkers, bij een bank, verzekeringsmaatschappij of ministerie. Ze houden zich bezig met het opsporen van witwaspraktijken, onderzoeken dubieuze schadeclaims of proberen te voorkomen dat onze bewindslieden tijdens werkbezoeken gevaar lopen, door het screenen van risicopersonen. Een ict-afdeling hebben ze daarbij niet tot hun beschikking. Toch speelt hun werk zich in toenemende mate op het internet af, al was het alleen maar omdat de werkdruk toeneemt en er voor veldwerk geen budget is. Toch hebben ze geen van allen een technische achtergrond. Daarom zijn ze hier: om in twee dagen tools en websites te leren kennen waarmee ze hun speurwerk sneller kunnen doen.

Motorclubs

Van Roij wil zijn cursisten daarbij ook bewust maken van de gevaren die ze lopen op het internet. Hij wil ze inprenten dat ze niet zomaar de websites kunnen bezoeken van de personen die ze onderzoeken. Die zouden achterdochtig kunnen worden, wanneer ze tussen de webstatistieken van bezoekers elke dag de naam van dezelfde bank tegen zouden komen. Gelukkig bestaan er tooltjes die je verzoek om een bepaalde webpagina op te vragen kunnen omleiden via een anonieme proxy-server. Maar dan moet je er wel op tijd aan denken om je Google-search te onderbreken. Let verdomd goed op', zegt van Roij. 'Als je op een site komt waar herkenning mogelijk is, wil ik dat je dat

anoniem doet.' Om zijn cursisten te drillen heeft hij vanmiddag allemaal spannende opdrachten bedacht. Ze gaan in veel gevallen over leden van 'motorclubs'.

'Zoek deze afbeelding', zegt van Roij. De projector toont het logo van een motorclub. Even later vindt de bankmedewerker, die even daarvoor nog de fout inging door ongeanomiseerd te surfen, de gevraagde foto. Hij wijst naar het scherm van de Google-afbeeldingenzoeker. 'Zonder door te klikken!', zegt hij triomfantelijk. Even later, tussen twee opdrachten door, is hij in gedachten verzonken. Hij denkt aan alle websites van verdachte organisaties, die hij in het verleden ongeanomiseerd heeft bezocht. 'Ik kan er wel een paar bedenken.' Zijn hand bedekt zijn mond.

WayBack Machine

De projector toont een foto van een hond op het strand. De cursisten moeten uitzoeken wanneer de hond geboren is. Ze krijgen alleen de naam van de hond, en de voornaam van zijn eigenaar. Even later is niets te horen behalve het klikken van muizen. De cursisten turen strak gespannen naar hun schermen, sommige met blosjes op hun wangen. Iedereen wil de eerste zijn die de oplossing heeft gevonden. De winnaar krijgt een usb-stick met een softwareprogramma dat kan controleren welke bestandsacties er de laatste zes weken op een machine zijn uitgevoerd. Na negen minuten heeft de verzekeringsmedewerker als eerste de oplossing gevonden. 'Jij mag wat gaan drinken', zegt van Roij.

'Kijk wat je ziet. Denk aan wat je geleerd hebt', moedigt van Roij de overige cursisten aan. Voor het uitvoeren van de opdrachten moeten de cursisten zich allerlei handige sites herinneren, waarmee ze de afgelopen twee dagen, vaak voor het eerst, kennis hebben gemaakt. Zoals de WayBack-machine, een site waarmee je terug kan gaan in de tijd. Handig wanneer iemand zijn Hyves-pagina heeft geblokkeerd. De medewerker van de verzekeringsmaatschappij: 'In het verleden dacht ik in zo'n geval: dit spoor loopt dood.'

In twintig minuten een dossier

De WayBack Machine hoort bij een rijtje van vijf, dat de opsporingsmedewerkers volgens van Roij altijd moeten gebruiken bij het onderzoeken van een bedrijfswebsite en het samenstellen van een opsporingsdossier: de Kamer van Koophandel, spYderweb, domeinregistrator SIDN en het kadaster. Van Roij: 'De efficiëntie qua tijd is enorm, als je zo'n speurtocht uitvoert volgens een vaste opbouw. Binnen twintig minuten heb je zo een startdossier bij elkaar gezocht.'