DIGITALE OPSPORING

Financiële fraudes zijn in de groeiende datastromen met enorme transactievolumes steeds moeilijker op te sporen. Kunstmatige intelligentie steekt een helpende hand toe. ‘Fraudes worden steeds slimmer en moeilijker detecteerbaar. Je mag niet stilstaan als je die succesvol wil bestrijden.’

Het algoritme als financiële speurneus

Martijn de Meulder

Data scannen met algoritmes zorgt voor minder foute meldingen en verlicht daardoor de werklast van de controle.
ILLUSTRATIE: GETTY IMAGES/FD STUDIO

Het Tripolis-gebouw aan de Amsterdamse Zuidas oogt desolaat: de gevels zijn gestript, het centrale plein is een grote, stoffige bouwput. Toch vervult dat uitzicht Joost van Houten met plezier. ‘Dit gaat echt fantastisch worden’, wijst hij met een breed armgebaar vanuit het kantoor van zijn fintechbedrijf Slimmer AI. ‘Uber gaat hier zijn hoofdkantoor vestigen en het plein wordt een overdekte campus. Veel kleinere start-ups hebben belangstelling. Dit wordt de techhub van de Zuidas.’

Van Houten is een van de huurders van het enige Tripolis-gebouw dat nog niet is gestript. Zijn kantoor kijkt uit over wat nu nog vooral een vastgoedbelofte is. Het is een aardige analogie met de wereld waarin hij werkt: die van de algoritmische opsporing van financiële misdaad. Want ook daar wordt op dit moment heel hard gebouwd aan de wereld van morgen. De eerste contouren zijn al zichtbaar. Dat was voor het kunstmatige-intelligentiebedrijf — vijftig man sterk, een decennium geleden ontstaan in de schoot van de Universiteit van Groningen — vorig jaar reden om een draai te maken: van consultant werd het een leverancier van algoritmes voor de beveiliging van financiële transacties.

ALGORITMISCH OPSPOREN

Die wending bleek al snel veelbelovend. Slimmer AI haalde in mei voor zijn fraudedetectiesoftware Sentinels een investering binnen van €4 mln bij een club ondernemers afkomstig van Bol.com, Booking.com en betaalverwerkers Adyen en Mollie. Want de algoritmische opsporing van criminelen maakt op dit moment een grote vlucht, legt Van Houten achter zijn MacBook uit.

Op zijn scherm laat hij een testopstelling zien met een rij aan verdachte transacties die door het algoritme uit de datastroom zijn geplukt en nader onderzoek behoeven. Algoritmes bestaan natuurlijk al veel langer en worden ook al door betaalverwerkers gebruikt. Maar tot nu toe waren het vooral *business rules*, zo legt Van Houten uit: een set van redelijk eenvoudige regels die een grove schifting van data kunnen verzorgen. Ze halen bijvoorbeeld alle transacties boven een bepaald bedrag uit de datastroom en geven deze door aan menselijke controleurs.

Maar de wereld is in hoog tempo complexer aan het worden. De mondiale transactievolumes worden ieder jaar groter. En er worden hogere eisen gesteld aan transactieverwerkers en financiele instellingen. Dat zorgt bij elkaar voor exponentieel meer data, tot een niveau dat niet meer te verwerken valt. Anderzijds wordt rekenkracht goedkoper en de ontwikkelingen in de cloud en kunstmatige intelligentie worden sneller. Van Houten: ‘Dan kom je al snel tot een eenvoudige conclusie. De betere gereedschappen die we nodig hebben om de datastromen aan te kunnen en financiële fraude tegen te gaan, die zijn er nu.’

Oprichter Adriaan Mol, van de Amsterdamse betalingsverwerker Mollie, is niet alleen investeerder, zijn bedrijf is ook *launching customer* van Slimmer AI. Mollie verwerkt jaarlijks voor meer dan €5 mrd aan betalingen voor zijn klanten. ‘Die passeren nu allemaal ons algoritme’, vertelt Van Houten. Na de eerste maanden in productie, zijn de effecten al merkbaar.

Een slim algoritme houdt rekening met de context waarbinnen een transactie wordt gedaan. ‘Dat zagen we het afgelopen Suikerfeest bijvoorbeeld. Dan

8

EEN SLIM ALGORITME HOUDT REKENING MET DE BREDERE CONTEXT WAARBINNEN TRANSACTIES WORDEN GEDAAN

Gerrie Lenting
Deloitte

‘VROEGER ZATEN WE ACHTER STAPELS DOSSIERS DE ADMINISTRATIE VAN BEDRIJVEN DOOR TE ZOEKEN NAAR FRAUDE. NU ZOUDEN WE NIET MEER ZONDER TECHNOLOGIE KUNNEN’

Joost van Houten
Slimmer AI

‘DE BETERE GEREEDSCHAPPEN DIE WE NODIG HEBBEN OM DE DATASTROMEN AAN TE KUNNEN EN FINANCIËLE FRAUDE TEGEN TE GAAN, DIE ZIJN ER NU’

7

worden er veel donaties gedaan aan lokale religieuze instellingen.’

De business rules gaven alerts af voor al die instellingen, ze kregen immers veel meer transacties te verwerken dan normaal. Het algoritme kijkt veel breder naar de terugkerende aard van dit soort transacties, naar wat voor ontvanger het is, hoelang deze bestaat, wat er bij vergelijkbare ontvangers gebeurt, en wie erachter zitten.

Als je daar rekening mee houdt krijg je veel minder *false positives*: meldingen die op fraude lijken maar het niet zijn. Tegelijk ontdek je juist patronen die zich aan klassieke fraudedetectievormen onttrekken. Van Houten: ‘Dat is wat je wil: de werklast voor de mensen die het uiteindelijke controlewerk moeten doen verlichten door betere data aan te leveren. En voorkomen dat fraudeurs een kans krijgen, met alle ethische, publicitaire en mogelijk strafrechtelijke gevolgen van dien.’

KEN JE KLANT

Onder financiële instellingen zijn de termen KYC (*know your customer*) en CDD (*customer due diligence*) de laatste jaren snel belangrijker geworden. Niet vreemd, want niet alleen de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) stelt hoge eisen aan transactieverwerkers en banken op het gebied van witwassen, fraude en terrorismefinanciering. Ook enkele grote schandalen in de afgelopen jaren hebben de financiële instellingen wakker geschud. Zo moest ING in 2018 voor €775 mln met het openbaar ministerie schikken vanwege zijn niet optreden tegen witwassen. Sinds eind vorig jaar staat ABN Amro centraal in een lopend witwasonderzoek van het openbaar ministerie.

Mede om die reden zijn de KYC en CDD-afdelingen van banken de afgelopen jaren explosief gegroeid. Maar de benodigde fraudespecialisten zijn nauwelijks te vinden, er staan honderden vacatures voor deze expertise bij de banken open. Niet vreemd dus dat geavanceerde algoritmes uitkomst bieden.

Fintechstart-ups zoals Slimmer AI of het Leusdense Fraud Dynamics leveren naar eigen zeggen algoritmes die de transactiestromen van banken realtime screnen. ‘We zijn inmiddels uit de pilotfase’, zegt Fraud Dynamics-oprichter Sjoerd Slot. ‘De processen bij banken zijn traag en uiteindelijk moet een algoritme zich eerst in de praktijk bewijzen. Maar ik heb geen enkele twijfel dat dat gaat lukken.’ Slot wijst erop dat tegenwoordig zoveel rekenkracht beschikbaar is dat letterlijk honderdduizenden factoren kunnen worden meegenomen in het opstellen van een algoritme. Dat is ook nodig, want fraudes worden steeds slimmer en moeilijker detecteerbaar in een groeiende stroom transacties. Slot: ‘Je mag niet stilstaan als je die succesvol wil bestrijden.’

De komst van geavanceerdere hulpmiddelen die nodig zijn om boeven op te sporen kan rekenen op bijval van de Nederlandse Vereniging van Banken (NVB). In zijn inventarisatie ‘Artificiële intelligentie in de financiële sector’ noemde de NVB in januari de komst van dit soort technieken zelfs onderdeel van ‘de vierde industriële revolutie’. ‘Maatschappelijk zal AI een belangrijke rol spelen bij de democratisering van diensten en producten, bij de bestrijding van financiele criminaliteit en bij de poortwachtersfunctie van banken.’ De vraag is volgens de NVB niet óf de technologie die nu wordt ingezet een opmars maakt, maar hóé dat gebeurt.

Ook Gerrie Lenting, hoofd van de Europese afdeling Forensic & Financial Crime bij accountants- en adviesmultinational Deloitte, zag de afgelopen decennia een enorme verandering: ‘Vroeger zaten we achter stapels dossiers de administratie van bedrijven door te zoeken naar fraude. Dat was klassiek forensisch accountancywerk. Tegenwoordig bestaat meer dan de helft van ons team uit econometristen, datawetenschappers en algoritme-experts en loopt het werk 24 uur per dag door. We zouden echt niet meer zonder technologie kunnen.’

REALTIMECONTROLE

Eenmaal per jaar de boeken controleren is allang niet meer genoeg, vertelt hij: ‘Stel je hebt een groot boekingsplatform voor reizen, daar vinden 24 uur per dag, zeven dagen in de week, transacties op plaats. Als je daar grootschalige fraude wil ontdekken moet je wel realtime controleren.’ Dat laatste stelt enorme eisen: het gaat niet alleen om afwijkende transacties, maar nadrukkelijk ook om transacties die zo op het eerste gezicht in orde lijken. Fraudes worden steeds slimmer en proberen zich te verschuilen in de legitieme datastroom. Die kunnen alleen ontdekt worden door nog slimmere detectiemechanismen.

Louter en alleen de transactie bekijken is te beperkt, aldus Lenting. ‘Context is alles in deze discipline. Hoe meer databronnen je hebt en hoe beter je associaties tussen verschillende handelingen in verschillende systemen kunt leggen, hoe beter je algoritme wordt.’ De kans op succesvolle opsporing wordt bijvoorbeeld veel groter door te bekijken wat er bij de bank vooraf en na de transactie gebeurt, of hoe de mensen achter de transactie daarover communiceren.

Het opent ook de poort naar scenario’s waarin kunstmatige intelligentie meer van ons af weet dan wij van onszelf en de privacy in het geding komt. ‘Er zijn natuurlijk grenzen aan hoeveel databanken je kunt en moet willen koppelen’, stelt Lenting. ‘Maar voor financiële of boekhoudkundige fraude geldt nu eenmaal dat meer data beter is. Je moet buiten de silo kunnen kijken waarin je werkt.’

Het opgeven van een deel van je privacy kan volgens hem ook gekoppeld worden aan privileges, zoals een efficiëntere transactieafhandeling en een veiligere betaal- en werkomgeving. ‘Ik denk dat dit de overweging waard is. Dat is een discussie die we met zijn allen moeten voeren, want dat deze technologie integraal onderdeel wordt van onze toekomst, dat is zeker.’

Martijn de Meulder
is freelancejournalist.

Slimme algoritmes sporen financiële fraude op als een moderne Sherlock Holmes.
ILLUSTRATIE: ISTOCK

€4 mln

Slimmer AI haalde al snel 4 miljoen euro bij investeerders op voor de ontwikkeling van de fraudesoftware.

ALGORITMES EN KUNSTMATIGE INTELLIGENTIE

De inzet van kunstmatige intelligentie bij het opstellen van algoritmes om financiële criminelen te pakken klinkt reuze mysterieus, maar het is minder ingewikkeld dan het lijkt.

Zo is een algoritme niet meer dan een serie regels om bijvoorbeeld een financiële transactie mee te beoordelen. Dat kan iets eenvoudigs zijn als: als het bedrag x euro hoger is dan de gemiddelde transactie van deze persoon, en deze transactie vindt plaats na tien uur ’s avonds dan kan deze verdacht zijn.

Dit soort klassieke algoritmes zijn nu al volop in gebruik. Kunstmatig intelligente software — wat in essentie ook niet meer is dan een verzameling algoritmes — kan echter ook worden gebruikt om zelfstandig dit soort algoritmes op te stellen. Dat doet het door met een door mensen opgestelde waardeset, zoals bovenstaande ‘als-danregel’, een enorme berg historische data door te ploegen.

De resultaten hiervan worden weer door mensen beoordeeld op wat een goed resultaat is en wat niet, waarna de kunstmatige intelligentie opnieuw door de databerg kan gaan, en nog betere gegevens oplevert.

Op die manier wordt het systeem getraind om immer betere algoritmes te produceren. Ga je die loslaten op nieuwe data, en koppelen met extra data, dan wordt het algoritme steeds ‘intelligenter’ en beter. Die intelligentie bestaat vooral uit geavanceerde patroonherkenning. Van echt intelligente machines is in deze wereld voorlopig nog geen sprake.