Equens bestrijdt skimmen met computerkracht

Helemaal voorkomen kan nog niet, maar Equens en wetenschappers van de Vrije Universiteit Amsterdam (VU) hebben een methode ontwikkeld die skimmen een stuk minder aantrekkelijk maakt. Daarbij spelen computerpower en inventiviteit een belangrijke rol.

Door de detectiemaatregelen is het gemiddelde schadebedrag van een geslaagde skimoperatie gedaald van 1500 naar 1100 euro. FOTO: ANP

De schade van skimmen bedroeg vorig jaar 36 miljoen euro, volgens de Nederlandse Verenging van Banken (NVB). En dat is 16 procent meer dan in het jaar ervoor. Wel is door detectiemaatregelen de schade per geskimde kaart in 2009 afgenomen van 1500 euro (in 2008) naar 1100 euro.

Equens, dat onder meer betalingstransacties van bankpassen en creditcards verwerkt, werkt nu ruim een jaar met een methode die gebruikmaakt van onder meer neurale netwerken en "een mix van andere technieken", die een razendsnelle fraudedetectie oplevert. Als banken dan snel ingrijpen door geskimde pasjes en/of de geskimde betaalautomaat of geldautomaat te blokkeren, hebben de criminele bendes die hierachter zitten minder tijd om de gekopieerde data van de pasjes te gebruiken. Daarmee wordt skimmen voor hen minder aantrekkelijk, in elk geval in Nederland, zo hoopt Equens.

De nieuwe fraudedetectiemethode heeft Equens ontwikkeld in nauwe samenwerking met het Fraude Detectie Expertise Centrum van de VU. Beide organisaties werken al vijftien jaar samen op het gebied van risicodetectie. Eerder werd door de VU en Equens al een detectiemethodiek voor creditcardfraude ontwikkeld. Daarbij wordt het profiel van een klant gematcht met het profiel van de transactie en dat van de 'merchant'. De profielen van klanten zijn maatwerk en geheel individueel. Voltrekt zich bijvoorbeeld een transactie die niet in dat profiel past, dan is dat alarmerend en kan dit op fraude wijzen. Zoals een commissaris van de koningin ondervond, die voor zijn vrouw een sieraad wilde kopen bij de juwelier. Dat deed hij echter nooit, waardoor het detectiesysteem dit zo verdacht vond dat zijn creditcard werd geblokkeerd.

Skimmen richt zich niet op een individuele pashouder maar op groepen; er worden al snel vijftig tot honderd kaarten geskimd op een betaalautomaat. Daarom zijn bij de methoden voor fraudedetectie ook regels voor groepsgedrag toegevoegd. De kennis van het gedrag van skimmers is afkomstig van Equens, die deze beroepsgroep inmiddels al jaren volgt. Prof. dr. Bert Kersten, hoogleraar Bedrijfswiskunde aan de VU: "Het is erg krachtig. Er worden relatief weinig foute beslissingen genomen doordat er meer regels in zijn opgenomen. Niet alleen statistieken maar ook menselijke factoren. De fraudeanalisten van Equens weten hoe bendes werken. Het is teamwork. Equens heeft veel kennis van het domein en wij van 'mining large data streams'. Je kunt dit niet alleen."

Maar de vele regels van het systeem alleen volstaan niet. Vindt er bijvoorbeeld een geldopname plaats in Boekarest terwijl diezelfde dag ook met de bankpas in Nederland wordt betaald, dan concludeert het detectiesysteem dat dit zeer onwaarschijnlijk gedrag is. Zoals een directeur van een grote multinational merkte die in Breda woonde, daar tankte op weg naar het vliegveld in Zaventem, vanwaar hij vertrok naar Mexico, alwaar hij die avond na aankomst geld wilde opnemen. Zijn pas werd echter geblokkeerd omdat dit gedrag onwaarschijnlijk was. Juist om dergelijke 'false positives' te voorkomen, kijkt er altijd nog een mens naar mogelijk alarmerende situaties. Het kan namelijk altijd ook nog te verklaren zijn.

Maar twee personen die afzonderlijk maar na elkaar in een tuincentrum betalen en beide in Parijs na twee uur een flink bedrag opnemen bij een geldautomaat, zijn wel heel duidelijke slachtoffers van skimmers. En die gegevens weet het systeem binnen 30 seconden te matchen. Daarbij heeft Equens de beschikking over één miljard transacties die voor detectie beschikbaar zijn. Daarin kunnen fraudeanalisten vrijuit grasduinen en alle mogelijke analyses laten maken.

Dat vereist wel zeel veel rekenwerk, benadrukt dr. Wojtek Kowalczyk, senior onderzoeker en wiskundige en informaticus aan de VU. En dat kan weer het beste door optimaal gebruik te maken van de groeiende computerkracht, zowel in snelheid als in geheugen. Kowalczyk is verantwoordelijk voor de ontwikkeling van algoritmen waarmee dit rekenwerk ook nog eens heel snel kan worden uitgevoerd. "Wij worden pas enthousiast als het op zijn minst om miljoenen transacties gaat", zegt hij. "Je kunt met wiskundige berekeningen voorspellen of iets fraude is of niet." Kersten benadrukt dat het optimaal gebruik van computerkracht bittere noodzaak is. Hij voorziet een voortgaande enorme groei van de hoeveelheid data. "Bedrijven en overheden slaan elk jaar twee keer zoveel data op als het jaar daarvoor. Probleem daarbij is dat

Gegevens van één miljard transacties geanalyseerd om skimmers te detecteren

bij veel organisaties het overzicht over die data afneemt." Maar niet bij Equens, benadrukt hij.

De één miljard transacties die worden gebruikt om skimmers te detecteren, zijn afkomstig van alle betaalautomaten in Nederland. Die moeten daarvoor allemaal gemonitord worden. Nu nog komen de gegevens in batches, maar straks moeten ze realtime worden geanalyseerd. De berekeningen moeten zodanig worden georganiseerd dat alles heel snel berekend kan worden. Kowalczyk: "Dat kan alleen met RAM-geheugen. Dat is één miljoen keer sneller dan harde schijven. Het betekent dat we elk willekeurig element in een stap kunnen gebruiken." Daar komt bij dat de prijs van RAM-geheugen de afgelopen jaren fors is gedaald terwijl de capaciteit erg groot is geworden. Een zwaar werkstation volstaat daarom voor de analyses op de één miljard transacties.

Op die miljard transacties kun je elke vraag loslaten. In een fractie van een seconde is de analyse gemaakt. In 30 seconden worden alle transacties van de laatste minuten geanalyseerd ten opzichte van alle voorgaande transacties. Drs. Eric Luijks, general manager Risk Management bij Equens: "Analisten beoordelen het en is het mis, dan laten ze dat de bank van de klant weten, die zelf bepaalt of hij ingrijpt door passen en/of betaalautomaten te blokkeren. Wij kunnen het ook doen; dat hangt af van het mandaat dat wij van de betreffende bank hebben gekregen." Alles snel blokkeren bij de geringste twijfel is ongetwijfeld het veiligst. Daarbij wordt echter een afweging gemaakt tussen de kosten en het ongemak die dat met zich meebrengt: blokkeren kost de bank geld, maar niet blokkeren ook.

Equens neemt een centrale positie in bij de bestrijding van fraude met betalings-transacties. Aanvallen worden immers zonder onderscheids des banks gedaan; ze treffen alle banken. Luijks: "En wij zien bijna alle transacties en monitoren die. Daarnaast hebben wij een liaisonfunctie met politie en justitie." Zijn afdeling telt 45 fte's, waarvan 13 zich bezighouden met fraudebestrijding en detectie.

Equens gebruikt nu ruim een jaar de nieuwe detectiemethode. De resultaten zijn verheugend. Luijks: "Bijna alle betaalautomaten die gemanipuleerd zijn, hebben we ontdekt. Ook zijn de passen sneller geblokkeerd dan voorheen. "Ook is de laatste maanden een afname te zien van skimmingaanvallen. Of dat aan het fraudedetectiesysteem ligt, is echter niet te zeggen. "Er worden ook andere maatregelen getroffen door de banken."

Daarnaast verwacht Equens dat de schade kleiner wordt. Luijks: "Bij de proof-of-concept is berekend dat we de directe schade kunnen beperken met 70 tot 80 procent als we 7 x 24 uur monitoren. Dat moet zich nog bewijzen omdat we nog in batchverwerking zijn. Zodra we overstappen op 7 x 24 uur, realtime verwerking, moet dat blijken." Skimmen tegenhouden zal niet lukken. Luijks: "We kunnen alleen detecteren en reageren maar dan is het al gebeurd. Maar door snel hun lijntjes door te knippen, kunnen we ze in elk geval frustreren."

Tanja de Vrede/t.vrede@sdu.nl