Nederlandse Vereniging van Banken

INTEGRALE AANPAK

Position Paper NVB

Digitale criminaliteit is een maatschappelijk probleem. Het leidt niet alleen tot persoonlijk leed bij gedupeerden, het ondermijnt ook het vertrouwen van de burger in het zakelijke verkeer. Criminelen maken steeds vaker misbruik van mogelijkheden om met digitale dienstverlening mensen op te lichten en fraude te plegen. Deze ontwikkeling zet door: ook klanten van banken zien zich in toenemende mate geconfronteerd met de risico's van digitale criminaliteit, waaronder fraude.

Banken nemen hun publieke taak uiterst serieus en vinden het verschrikkelijk om te zien dat veel klanten de dupe worden van digitale criminaliteit. Ze willen dit graag oplossen, maar kunnen dit niet alleen. Banken dringen er daarom met grote klem op aan om snel invulling te geven aan de toezegging van minister Hoekstra uit december 2020 om "samen met de minister van Justitie en Veiligheid en de banken, te onderzoeken hoe we de samenwerking op het gebied van fraudebestrijding nog verder kunnen vormgeven en hoe we die fraudebestrijding nog meer kunnen versterken." Verder uitstel betekent meer schade voor slachtoffers en criminelen die nog langer hun gang kunnen gaan.

Banken bepleiten een integrale aanpak, waarbij alle betrokken partijen, onder regie van de overheid, nauw met elkaar samenwerken. Dit betreft ministeries, toezichthouders, politie, Openbaar Ministerie, banken, sociale media, BigTech's, Internet Service Providers, telecompartijen en handelsplatformen. Deze aanpak zou heel snel, en veel sneller dan nu het geval is, moeten leiden tot intensieve samenwerking waarin al het mogelijke gedaan wordt om de fraudecijfers naar beneden te krijgen.

We willen de overheid nadrukkelijk aansporen tot actie, omdat de overheid kan wat wij als sector alleen niet kunnen, namelijk:

1. ***Zorgen voor commitment van alle betrokken partijen,***
2. ***Barrières wegnemen om gegevens te delen tussen de genoemde partijen,***
3. ***Investeren in betere digitale vaardigheden van burgers,***
4. ***Verhogen van de pakkans en intensiveren van de vervolging van cybercriminelen en***
5. ***Het vrijmaken van voldoende middelen om dit effectief te kunnen doen.***

Een integrale aanpak van digitale criminaliteit, waarin deze punten worden meegenomen, verdient prioriteit van een nieuw kabinet. Nieuw beleid en allocatie van extra middelen is noodzakelijk, zoals ook is geadviseerd door de Cyber Security Raad. [1]

[1] https://www.cybersecurityraad.nl/actueel/nieuws/2021/04/06/csr-adviseert-%E2%82%AC833-miljoen-voor-een-integrale-aanpak-voor-cyberweerbaarheid

➢ *Context*

Online werken, onderwijs volgen en winkelen is tegenwoordig de normaalste zaak. Ook het onderhouden van sociale contacten en het doen van betalingen gebeurt hoofdzakelijk online. Dit heeft vele voordelen, maar de voortschrijdende digitalisering leidt tegelijkertijd tot een stijging van digitale criminaliteit. De totale schade als gevolg van phishing (6,1 miljoen euro) en bankhelpdeskfraude (16,5 miljoen euro) kwam in de eerste zes maanden van 2021 uit op ruim 22,5 miljoen euro. Ter vergelijking: de totale schade van deze vormen van digitale criminaliteit bedroeg in heel 2020 39,5 miljoen euro. De schade loopt daarmee verder op naar een zorgwekkend hoog niveau.

Ook klanten van banken zien zich in toenemende mate geconfronteerd met de risico's van digitale criminaliteit. Slachtoffers worden gebeld of krijgen een sms, ze ontvangen een bericht via Whatsapp of e-mail of ze worden opgelicht bij een aankoop via een digitaal platform. Succesvolle digitale criminaliteit loopt ook steeds vaker via verschillende kanalen tegelijk, criminelen professionaliseren en combineren hun misdaad soms met een fysiek bezoek. Criminele organisaties zijn zeer innovatief en flexibel. Ze veranderen steeds sneller van methodes en zijn de slachtoffers en partijen in de keten daarom geregeld te snel af. Het doel is vrijwel altijd hetzelfde; mensen verleiden om zelf geld over te maken of de toegang te openen tot de bankomgeving.

De bankensector blijft innoveren en investeren in een veilig en betrouwbaar betalingsverkeer. Banken vinden dit belangrijk en zijn hier altijd op aanspreekbaar. Ondanks de technische maatregelen om fraude terug te dringen en hun inspanningen om consumenten voor te lichten en te waarschuwen zien banken digitale criminaliteit toenemen. Banken kunnen deze problematiek niet alleen oplossen.

➢ *Een integrale aanpak is nodig*

De bestrijding van digitale criminaliteit schiet tekort. Het ontbreekt aan een gezamenlijke strategie en de opsporing van criminelen wordt gehinderd door belemmeringen ten aanzien van het delen van informatie tussen bijvoorbeeld banken en politie. De pakkans voor criminelen is laag. Kwetsbare groepen beschikken ondanks voorlichtingscampagnes nog altijd niet over voldoende digitale vaardigheden.

Alleen in gezamenlijkheid, dus met medewerking van alle betrokken publieke en private partijen, kan een vuist tegen digitale criminaliteit worden gemaakt. Er wordt al veel gedaan en dat is niet zonder effect. De huidige samenwerking is echter vaak ad-hoc, waardoor het vaak een tijdelijk karakter heeft. Ook is de samenwerking vaak gericht op een specifieke vorm van digitale criminaliteit. Als een vorm van digitale criminaliteit geïsoleerd wordt aangepakt treedt een 'waterbedeffect' op: criminelen ontwikkelen een nieuwe vorm van criminaliteit.

Bij het formuleren van een gemeenschappelijke strategie en het voeren van regie dient waar mogelijk te worden aangehaakt bij bestaande structuren en samenwerkingsverbanden. Een voorbeeld van een samenwerkingsverband is de ECTF (Electronic Crimes Taskforce), waarin banken, politie en OM samenwerken bij de aanpak van gedigitaliseerde financiële criminaliteit. Samenwerking met de Vereniging COIN heeft geleid tot succesvolle initiatieven in het tegengaan van phishing via sms (smishing) en telefonie (met nummerspoofing).

➢ *Hoofdlijnen integrale aanpak*

De banken zien voor de integrale aanpak vijf speerpunten:

1. Commitment van alle betrokken partijen, waarbij voor een langere termijn mensen en middelen beschikbaar worden gesteld. De overheid heeft een rol om partijen bij elkaar te brengen en partijen erop te wijzen dat zij onderdeel zijn van de oplossing.
2. Barrières wegnemen om gegevens te delen tussen de betrokken partijen (data ten behoeve van detectie, preventie, opsporing en vervolging tussen banken onderling, de overheid en andere sectoren). Banken lopen daar tegenaan in hun onderlinge contacten, in contacten met ketenpartners en in de samenwerking met publieke partijen (OM/politie). Dit vraagt om aanpassingen van privacy- en eventueel andere nationale en internationale wet- en regelgeving, zoals de Telecomwet. Meer in het algemeen is het belangrijk om kennis en

inzichten over digitale criminaliteit onderling uit te wisselen. Ook de mogelijkheden om criminelen op te sporen en aan te pakken haperen door knellende (privacy)wetgeving. Een vergunningsaanvraag bij de Autoriteit Persoonsgegevens (AP) om interbancair gebruik te kunnen maken van de wettelijke mogelijkheden tot gegevensuitwisseling is complex en de afhandeling duurt te lang. Dit vraagt om verbetering.

3. Investeren in betere digitale vaardigheden. Betrokken partijen tonen op dit gebied uiteenlopende initiatieven. Meer samenwerking en afstemming is dringend gewenst om te komen tot een lange termijn communicatiestrategie. Die zou zich moeten richten op voorlichting via een breed palet aan media en zich moeten richten op diverse doelgroepen. Deze strategie zou m.m.v. alle relevante partijen tot stand moeten komen, waarbij onder regie van de overheid met name een zichtbare rol van de telecomsector en Internet Service Providers gewenst is.
4. Verhogen van de pakkans en intensiveren van de vervolging van cybercriminelen (ook internationaal). De bestaande vormen van Publiek-private samenwerking hebben hun toegevoegde waarde bewezen maar kunnen nog effectiever opereren. Met name de Electronic Crimes Taskforce en het Landelijk Meldpunt Internetoplichting (LMIO; banken, OM, politie en Marktplaats) hebben nog veel potentieel. Ook aanpassingen binnen de politieorganisatie zelf kunnen bijdragen aan een succesvolle opsporing. Banken pleiten voor een sterkere focus van cybercrimeteams en (gewone) recherche op fraude en voor een goed gecoördineerde, eenheidoverstijgende landelijke aanpak voor de opsporing van cybercriminelen.
5. Voldoende middelen vrijmaken om dit effectief te kunnen doen. Veel van de benodigde acties zijn te vertalen in investeringen in mensen en middelen, die voor een langere termijn beschikbaar worden gesteld.

➢ ***Wat is op korte termijn nodig?***

Voor een snelle start van de integrale aanpak van digitale criminaliteit dienen alle partijen bestuurlijk commitment te geven en gezamenlijk daadwerkelijk tot concrete acties te komen om de alsmaar stijgende digitale criminaliteit het hoofd te bieden. Kortom er moet een breed pact wordt gesloten tegen oplichters.

Voor een snel begin met de integrale aanpak is op korte termijn het volgende nodig:

- Een bestuurlijk overleg met vertegenwoordigers van de ministeries van Justitie en Veiligheid, van Economische Zaken en Klimaat en van Financiën, toezichthouders (AP), politie, Openbaar Ministerie, banken, sociale media, BigTech's, Internet Service Providers, telecompartijen en handelsplatformen. Tijdens dit overleg kunnen er afspraken worden gemaakt over doelstellingen en vormen van samenwerking.
- Een gezamenlijke publieke verklaring waarin bestuurlijk commitment wordt uitgesproken. Dit commitment richt zich op het realiseren van een integrale aanpak van digitale criminaliteit en moet leiden tot een actieplan. Hierin moeten enerzijds korte termijn acties worden benoemd en anderzijds acties gericht op het creëren van voorwaarden voor een duurzame, lange termijn, strategische samenwerking tussen publiek en private ketenpartijen. Banken willen ook benadrukken dat digitale criminaliteit niet ophoudt bij de landsgrenzen. Daarom zullen de strategische doelstellingen zich niet alleen op landelijke samenwerking maar ook op een Europese aanpak moeten richten.
- Oprichting van een gezamenlijke stuurgroep waarin alle betrokken partijen zijn vertegenwoordigd.

Quick wins;

- Oprichting van een landelijk centraal aangiftepunt
- Oprichting van een opsporings/quick response team

Een snelle start aan de integrale aanpak is noodzakelijk. Verder uitstel van deze gezamenlijke bestrijding van digitale criminaliteit betekent dat de kans blijft liggen om maatregelen te nemen die slachtoffers en schade kunnen voorkomen.

➢ *Slot*

De digitalisering van het dagelijks leven zal verder toenemen. Dit brengt hogere risico's op digitale criminaliteit met zich mee, onder andere in het betalingsverkeer. Banken zien een zeer sterke stijging van digitale criminaliteit en willen dit graag oplossen, maar kunnen dit niet alleen. Daarom is een integrale aanpak noodzakelijk, waarbij alle betrokken partijen onder regie van de overheid nauw met elkaar samenwerken. Dit is ook in lijn met de het adviesrapport "Integrale Aanpak Cyberweerbaarheid 2021" van de Cyber Security Raad.

De banken nemen hun verantwoordelijkheid door te blijven investeren in beveiliging en voorlichting van hun klanten. Banken bepleiten met name aanpassingen in privacywetgeving om de opsporing van criminelen te vergemakkelijken, meer publiek-private samenwerking op dit vlak en het alloceren van extra overheidsmiddelen voor de aanpak van cybercriminaliteit. Een snelle start van een integrale aanpak is noodzakelijk.

Contactinformatie

Agnieta van der Plaat
M +31 (6) 30 23 26 64
E vanderplaat@nvb.nl
www.nvb.nl