Projectgroep Aanpak digitale criminaliteit Oost-Nederland

Eindverslag

Eind 2017 organiseerden het Openbaar Ministerie en de politie 'keukentafelgesprekken' over het thema cybercrime. Daar ontstond het idee om samen met de gemeente Nijmegen een pilot te starten voor het uitwerken van een barrièremodel tegen accountovername [1]. Deze vorm van digitale criminaliteit komt vaak voor en heeft ook een grote maatschappelijk impact. Bovendien zijn er tijdens de verschillende fases van het criminele proces zowel preventief als repressief volop interventies mogelijk. Dat maakte het interessant om met de pilot te onderzoeken of er een maatschappelijke alliantie mogelijk zou zijn met ondernemers ten behoeve van *awareness* en preventie, waarvoor de Projectgroep aanpak digitale criminaliteit Oost-Nederland werd opgericht, bestaande uit vertegenwoordigers van het Openbaar Ministerie Arrondissementsparket Oost-Nederland, de Eenheid Oost-Nederland van de politie en de gemeente Nijmegen (afdeling Veiligheid).

Werkwijze

De hoofdactiviteiten van de projectgroep bstonden uit:

1. Het uitwerken van het barrièremodel.
2. Het voorbereiden en begeleiden van twee experrtsessies met fraude-experts van webshops en telecombedrijven, respectievelijk op 25 september 2018 en 19 februari 2019.
3. Het maken van een eindrapportage.

Deelnemers projectgroep

1. Marjoleine ten Velde (OM)
2. Martijn Simons (OM)
3. Martin Enderink (OM)
4. Corinne Slagman (politie)
5. Michiel Ras (politie)
6. Kristiaan Schuppers (politie)
7. Wim Engelen (gemeente Nijmegen)
8. Roy Winkelhuijzen (gemeente Nijmegen – trainee 1 april 2018 - 30 september 2018)
9. Marc Wieringa (gemeente Nijmegen – trainee 1 oktober 2018 - 31 maart 2019)

[1] Definitie accountovername: het hacken van gebruikersaccounts bij webwinkels en telecombedrijven met als doel het verkrijgen van goederen.

Het barrièremodel

Het criminele proces bestaat uit 7 stappen. Hieronder volgt een korte beschrijving van die stappen.

1. Verkrijgen van accountgegevens
   In deze fase is de crimineel op zoek naar alle gegevens van een account om mee in te kunnen loggen bij de webshop. Dit kan door de inloggegevens van het webshopaccount te achterhalen. Maar ook door de email te hacken, meestal via phishing of door hergebruik van op het (dark)web aangeboden credentials.

2. Inloggen
   Het inloggen op het gehackte webshopaccount. Het probleem is hier dat webshops niet kunnen vaststellen dat degene die in probeert te loggen niet de échte klant is, maar een crimineel (identiteitsfraude).

3. Gegevens aanpassen
   De hacker past de accountgegevens aan. Het gaat dan primair om het afleveradres. Verder ook om zaken als het telefoonnummer, emailadres of wachtwoord.

4. Bestellen
   De hacker plaatst de bestelling. Vaak gaat het om producten die veel geld waard zijn en makkelijk door te verkopen, bijvoorbeeld elektronica en dure kleren. Deze groep criminelen lijkt zich niet te specialiseren – ze pakken alles aan wat ze kunnen krijgen. Het lijkt erop dat criminelen, wanneer ze eenmaal inloggegevens hebben verkregen, op meerdere webshops proberen in te loggen en producten te bestellen. Hierbij worden soms ook op het oog willekeurige producten besteld, die niet echt waardevol zijn en niet of nauwelijks door te verkopen. Waarschijnlijk betreft het wel vaak “draagbare” zaken (geen koelkasten of 60 inch TV’s).

5. Betalen
   Het betalen van de bestelling via het account van het slachtoffer. Er wordt, voor zover bekend, minder gebruik gemaakt van gestolen creditcardgegevens en andere aan het account gekoppelde betaalaccounts. Gestolen creditcardgegevens worden meer gebruikt om nieuwe accounts aan te maken. Zelfs de grote webshops hebben slechts een laag percentage “high value accounts”, waar de creditcardgegevens van de klant aan gekoppeld zijn. Criminelen kiezen meestal voor achteraf betalen (het slachtoffer krijgt de rekening) of voor betalingen met tegoeden van de webshop die gekoppeld zijn aan het account.

6. Aflevering
   De goederen worden afgeleverd door de leverancier en door iemand (een katvanger of medeplichtige van de hacker) afgevangen. Bij webshops wordt meestal voor afleverpunten gekozen; bij telecomaanbieders meestal voor huisadressen. In het geval van huisadressen gaat het meestal om bestaande gewijzigde adressen (niet van de oorspronkelijke klant). Hierbij kan het pakket in sommige gevallen al worden afgevangen voordat het het adres bereikt (bijv. in portiekwoningen).

7. <u>Heling en witwassen</u>
   De gestolen goederen worden verkocht t.b.v. cash, of andere middelen. Hier hebben we weinig zicht op, maar het lijkt erop dat bestelde producten regelmatig via Marktplaats of Used Products worden verkocht. Daar worden soms ook gehackte accounts voor gebruikt, of accounts waaraan een e-mailadres of telefoonnummer is gekoppeld dat ook in de gehackte webshopaccounts wordt gebruikt.

Een volledige beschrijving van het barrièremodel met daarin ook een beschouwing van de mogelijke interventies is opgenomen in bijlage 1.

Hieronder de uitwerking van het barrièremodel tegen accountovername in een schema.

Stappen	1: Verkrijgen van gegevens	2: Inloggen	3: Aanpassen	4: Bestellen	5: Betalen	6: Afleveren	7: Heling/witwassen
Beschrijving	* Phishing * Hergebruik van op het (dark)web aangeboden credentials	Frauderen met account en identiteit van een ander	Wijzigingen doorvoeren in voorbereiding op bestellen.	In het algemeen dure, makkelijk te verkopen producten (elektronica en kleren)	* Achteraf betalen * Betalen met tegoeden * Creditcard * Paypal	* Op normale adres klant * Op ander adres * Nepadres * Afhaalpunt met/zonder identificeerplicht * Corrupte chauffeur	Producten worden in gebruik genomen of doorverkocht.
Interventies	Overheid: Creëren bewustwording bij burgers en bedrijven tegen onveilige wachtwoorden en phishing. **Totaal 7 (+10, -3, effect 2)**	Branche + webshops: Een online en betrouwbare manier introduceren om identiteit te verifiëren, bv. via de app IRMA. **Totaal 11 (+13, -2, effect 5)**	Webshop: Klant informeren wanneer verdachte wijzigingen zijn doorgevoerd. **Totaal 7 (+6, -1)**	Webshop: Meer beveiliging bij riskante producten, bv. door extra verificatieopties toe te voegen. **Totaal 5 (+7, -2)**	Webshops en betaalmaatschappijen: Monitoren en delen informatie over verdachte accounts voor achteraf betalen. **Totaal 6 (+8, -2)**	Webshop + leverancier: Goede samenwerking om (gevlagde) frauduleuze bestellingen te onderscheppen. **Totaal 8 (+10, -2, effect 3)**	Politie: Traceren gestolen goederen na gebruik, bv. op serienummer. **Totaal: 4 (+7, -3)**
	Webshops: Veilig opslaan klantgegevens (controlerende rol Autoriteit Persoonsgegevens) **Totaal 4 (+7, -3)**	Webshop: Tweestapsverificatie instellen bij inloggen in account (bv. via SMS). **Totaal 7 (+10, -3, effect 4)**	Webshop: Klant verdachte wijzigingen laten verifiëren via extra stap **Totaal 4 (+8, -4)**	Betaalmaatschappij: Tweestapsverificatie instellen bij plaatsen van (verdachte) bestelling (bv dmv IRMA, als die niet wordt gebruikt bij inloggen) **Totaal: 6 (+9, -3)**	Betaalmaatschappij/webshop: Klanten altijd in laten loggen bij betalen. **Totaal 5 (+10, -5, effect 4)**	Overheid: Bewustwording creëren bij burgers (senioren) over afvangers. **Totaal 3 (+6, -3)**	
	Webshop: eisen stellen aan wachtwoorden **Totaal 7 (+9, -2, effect medium)**	Webshops: Notificatie-email als er wordt ingelogd met een vreemd IP-adres of vanaf een vreemde locatie. **Totaal 7 (+8, -1, effect 2)**	Publiek-private samenwerking: monitoren verdachte gegevens en delen met elkaar. Werken met een soort zwarte lijst. **Totaal 3 (+8, -5)**	Webshop: Bestelgeschiedenis klant meenemen in risicoprofiel. **Totaal: 6 (+9, -3)**	Webshops: Strengere eisen stellen aan producten voor achteraf betalen (bv. tot 50% wél van tevoren betalen) **Totaal 3 (+9, -6)**	Webshop + leverancier: Werken met zwarte lijst van verdachte adressen. **Totaal 6 (+10, -4, effect 4)**	
	Webshops + politie: uitwisselen informatie m.b.t. lijsten met credentials op het (dark)web. **Totaal 3 (+6, -3)**					Politie: sneller verdachten oppaken (afvangers) of het gesprek aangaan, voor een afschrikwekkende werking. **Totaal 6 (+10, -4, effect 4)**	
	Emailmaatschappijen: Email extra beveiligen om te voorkomen dat fraudeur erin kan **Totaal 5 (+10, -5, effect 4)**					Postorderbedrijf: aanpakken interne fraude en corruptie van pakketbezorgers. **Totaal 5 (+9, -4)**	
						Afhaalpunt: Beter controleren op identiteit afhaler. **Totaal 7 (+9, -2, effect 3)**	

Legenda
Goede score
Mogelijk goede score
Redelijke score
Lage score

Vetgedrukt zijn de scores toegevoegd: het totaal (combinatie van de plus- en minpunten)

Indicatoren voor de scores in het schema

1. Effectiviteit (+5; wat is kracht van maatregel, 100% waterdicht of enigszins werend)
2. Draagvlak (+5; staan de betrokken partijen positief tegenover de interventie?)
3. Reikwijdte (+5; werkt het voor alle MO's of alleen voor alleen voor een specifiek sub-MO)
4. Praktische uitvoerbaarheid (-2)
5. Juridische uitvoerbaarheid (-2)
6. Betaalbaarheid (-2)
7. Realisatiesnelheid (-2)
8. Optelsom pluspunten
9. Optelsom minpunten
10. Optelsom totaal

Expertsessies

In de experrtsessies zijn we het gesprek aangegaan met de fraude-experts van van landelijke operende webshops en telecombedrijven. De deelnemerslijst is opgenomen in bijlage 2.

Als vertrekpunt voor het gesprek stonden 3 thema's centraal:

1. Detectie (potentiële) frauduleuze patronen bij inloggen, aanpassen van gegevens, bestellen/betalen, afleveren en heling.
2. Een veiligere methode gebruiken voor inloggen.
3. Frauderegister om verdachte gegevens (waarmee eerder is gefraudeerd) te vlaggen.

Hieronder is in het schema van het barrièremodel aangegeven hoe die thema's zich tot het model verhouden.

Stappen	1: Verkrijgen van gegevens	2: Inloggen	3: Aanpassen	4: Bestellen	5: Betalen	6: Afleveren	7: Heling/witwassen
Beschrijving	* Phishing * Kwetsbaar wachtwoordgebruik * Wachtwoordreset * Hergebruik van op het (dark)web aangeboden credentials	Frauderen met account en identiteit van een ander	Wijzigingen doorvoeren in voorbereiding op bestellen.	In het algemeen dure, makkelijk te verkopen producten (elektronica en kleren)	* Achteraf betalen * Betalen met tegoeden * Creditcard * Paypal	* Op normale adres klant * Op ander adres * Nepadres * Afhaalpunt met/zonder identificeerplicht * Achterhouden door chauffeur	Producten worden in gebruik genomen of doorverkocht.
Interventies	Monitoren van lijsten gehackte credentials op het (dark)web	Detectie (potentiële) frauduleuze patronen bij inloggen, aanpassen van gegevens, bestellen/betalen, afleveren en heling					
	Monitoring en uit de lucht halen phishingsites. Barrieres m.b.t. versturen phishingmail.	Notificatie naar klant bij verdachte inlogpoging	Notificatie naar klant bij wijziging in gegevens	Bestelmogelijkheden beperken op basis van type product, bestelgeschiedenis klant e.d.	Betaalmogelijkheden beperken op basis van type product, bestelgeschiedenis klant e.d.	Samenwerking tussen postorderbedrijf en leverancier om frauduleuze bestellingen te onderscheppen	Traceren van goederen na gebruik
	Eisen stellen aan wachtwoorden	Een veiligere methode gebruiken voor inloggen	Tweestapsverificatie bij wijzigingen	Tweestapsverificatie bij (mogelijk verdachte) bestelling	Tweestapsverificatie bij betalen	Betere identiteitscontrole bij afhaalpunten	
	Extra beveiligen email, om nieuwe wachtwoordaanvraag door fraudeur te voorkomen	Tweestapsverificatie bij inloggen			Restricties wat betreft achteraf betalen (bijv. slechts gedeeltelijk achteraf betalen)	Investeren op katvangers: preventief en repressief	
	Tweestapsverificatie bij wachtwoordreset					Voorkomen corruptie door chauffeur	
	Verhogen bewustwording bij consument	Frauderegister om verdachte gegevens (waarmee eerder is gefraudeerd) te vlaggen					

We beschrijven hieronder kort de belangrijkste inzichten die de expertsessies ons hebben gebracht.

Preventie versus repressie

De marktpartijen zijn van mening dat zij al veel barrières hebben opgeworpen en vroegen zich af hoe OM en politie hun rol nu willen invullen. Uit het gesprek hierover werd duidelijk dat OM en politie scherpe keuzes moeten maken, zodat ze met hun inzet ook echt een verschil kunnen maken. Alle informatie waarmee het hacken van gebruikersaccounts beter in beeld kan worden gebracht is hierbij welkom. Aangiftes door (grote) bedrijven zijn in dit kader van aanzienlijk belangrijk, omdat zij in potentie voor de politie veel waardevolle informatie kunnen opleveren. Er zijn in geval van aangiftes ook geen restricties in dat verband, bijvoorbeeld met het oog op privacy-overwegingen. Maar de politie kan niet altijd op voorhand aangeven wat met informatie wordt gedaan. Maar door alle ingekomen informatie te combineren krijgt zij criminele groeperingen beter in kaart. Wel onderkennen OM en politie het belang van terugkoppeling overwat er met de aangifte gebeurd is.

Het zou helpen als er (landelijk) één centraal politieteam zou zijn dat hiervoor het vaste aanspreekpunt is voor de grotere webwinkels en voor de telecombedrijven. Dan is ook het gesprek mogelijk over de vraag welke informatie relevant kan zijn om de politie ook echt vooruit te helpen (denk bijvoorbeeld aan: google-id's, ip-adressen, user agent strings, e-mailadressen, etc). Ook zou automatisering van het aangifteproces kunnen helpen om meer snelheid in het proces te brengen.

Pilotprojecten kunnen eveneens nuttig zijn om de samenwerking op gang te helpen. Zo ontstond het idee voor een *Pilot Heterdaadjes*, gericht op het aanpakken van de levering van frauduleuze bestellingen. Of een actie gericht op het in beeld krijgen van jeugdige daders, opdat de politie tijdig STOP-gesprekken kan voeren. Ook het aanleggen van een register met frauduleuze accounts kan een interessant initiatief zijn.

Preventie

In beginsel liggen er veel mogelijkheden voor preventie. Grosso modo zijn de 3 belangrijkste invalhoeken:

1. Voorlichting en educatie aan de consument.
   Veilig gebruik van internet blijft een aandachtspunt. Belangrijk is dat de jeugd op school hierover al voorlichting krijgt, in elk geval ten aanzien van basale noties als: tijdig wachtwoorden wijzigen, het belang van het gebruiken van meertrapsverificaties of het gebruik van een digitaal paspoort. Zou het niet helpen als er iets zou komen als een 'computerrijbewijs'? Hier ligt in elk geval een belangrijke taak voor de overheid. Webwinkeles en telecombedrijven zouden hun klanten periodiek kunnen wijzen op het belang om de inlogcodes te wijzigen.

2. Delen van informatie en trends
   We hebben te maken met een complex en lastig grijpbaar fenomeen. Willen we daar grip op krijgen, dan is het belangrijk om informatie (ook detailgegevens, denk hierbij aan: signalen) en trends actief te delen, zowel tussen overheid en bedrijven als tussen bedrijven onderling. Zo kunnen ook daderprofielen tijdig in kaart worden gebracht, waar bedrijven weer gebruik van kunnen maken. Een frauderegister kan helpen, maar de vraag is wie hiervoor verantwoordelijkheid draagt. De sector zelf, de overheid of zou het een publiek-private samenwerking moeten zijn? Dit is in de expertsessies onduidelijk gebleven.

3. Digitaal paspoort voor gebruik webwinkel
   Tijdens de eerste expersessie is de werking van de door de Radboud Universiteit Nijmegen ontworpen privacy app IRMA (I Reveal My Attributes) toegelicht. Zo'n applicatie werkt als een digitaal paspoort, wat een sluitende gebruikersauthentificatie tijdens het inloggen mogelijk maakt. Bedrijven geven aan dat zij het belangrijk vinden dat voor klanten geen onnodig hoge drempel wordt opgeworpen voor toegang tot webwinkels. Klantvriendelijkheid staat voor hun voorop. Een wettelijke verplichting om zo'n digitaal paspoort te gebruiken vinden zij dan ook niet wenselijk.

Wat kan het bedrijfsleven zelf?
Voor een deel zij we hier in bovenstaande al op ingegaan. Webshops en telecombedrijven hebben een verantwoordelijkheid in het bevorderen van fraudebestendigheid van hun diensten en producten. Daarbij is wel de vraag hoever die gaat, mede gelet op het feot dat de consument ook een verantwoordelijkheid heeft ten aanzien van veilig internetgebruik. Daarnaast zien we dat bij bedrijven de sensitiviteit ten aanzien van de laagdrempeligheid hoog is. Men wil niet het risico lopen dat de klant bij een concurrent gemakkelijker toegang heeft tot de de digitale winkel. Wat hierbij een rol speelt is dat er in dezde branche nog geen echte vorm van samenwerking is: er is geen brancheorganisatie die zich hard kan maken voor een gemeenschappelijk *level playing field*. Terwijl wel de overtuiging is dat ten aanzien van gegevensuitwisseling en het beveiligen van de gebruikersaccounts het bedrijfsleven wel gezamenlijk zou moeten optrekken.

Conclusies

Een barrièremodel tegen het hacken van gebruikersaccounts blijkt ingewikkelde vraagstukken met zich mee te brengen. Het is niet *one giant leap for mankind* [2], maar het is een kwestie van vele kleine stapjes. Meest voor de hand liggen de hierboven beschreven mogelijkheden voor de samenwerking tussen enerzijds OM en politie en anderzijds de grote webwinkels en telecombedrijven op het snijvlak van preventie en repressie. Maar die zal vooral op gang moeten komen met behulp van pilotprojecten. OM en politie in Oost-Nederland zullen hiertoe de contacten met de webshops en telecombedrijven warm houden.

Kijken we naar preventie dan ligt er voor de overheid een belangrijke taak bij het weerbaar maken van de burger. Voorlichting en educatie spelen hier een belangrijke rol, waarvoor op lokaal niveau kansen liggen in het onderwijs en in het maatschappelijk opbouwwerk. De landelijke overheid zou zich moeten bekommeren om kwesties ten aanzien van een digitaal paspoort. Is hiervoor een wettelijke regeling nodig, of laten we dit aan de markt? Verder is het belangrijk dat de landelijke overheid zich buigt over de vraag: welke eisen stellen we aan aanbieders van digitale dienstverlening met het oog op de zorgplicht ten opzichte van consumenten? Onze conclusie is dat hedt bedrijfsleven dit (nog) niet zelf kan, c.q. wil regelen.

Voor ons was een belangrijke vraag of er een maatschappelijke alliantie mogelijk zou zijn op basis van het ontwikkelde barrièremodel? Mede gelet op de voorgaande conclusies blijkt dat een stap te ver. De scoop is te groot, partijen staan nog te ver van elkaar af, er is nog te veel discussies over verantwoordelijkheden en over de vraag of die publiek dan wel privaat moeten worden belegd. Als er al afspraken mogelijk zijn (over de samenwerking op het snijvlak van preventie en repressie, of over de invoering van een digitaal paspoort), dan liggen die toch vooral op nationaal vlak. Maar veelal zal er toch ook sprake zijn van monosectorale stappen.

[2] Neil Armstrong tijdens de eerste maanlanding.

Bijlagen

1. Beschrijving hacking van webshopaccounts; onderdelen voor het barrièremodel.
2. Deelnemerslijst expertmeetings.