Stand van zaken Internetoplichting en cybercrime in 2023: situatie onverminderd ernstig, politie vraagt om extra middelen

Begin 2023 sprak ik een aantal deskundigen over oplichting via digitale middelen (gedigitaliseerde criminaliteit en cybercrime) en constateerde: het is code oranje, er wordt veel schade geleden en de kans dat de verantwoordelijke criminelen daarvoor gepakt worden is klein, ondanks de inspanningen die gepleegd worden om deze vorm van misdaad te voorkomen of te bestrijden. Dat was misschien geen erg positief beeld. Nu er inmiddels bijna een jaar verstreken is, haal ik het net opnieuw op, hoe staan de zaken er nu voor? Conclusie, er is zeker zoet, maar ook nieuw en oud zuur.

Gedigitaliseerde criminaliteit is het plegen van fraude en oplichting maar dan met digitale middelen, bij cybercrime zijn de digitale middelen zelf het doel zoals het toepassen van "ransomware" (computers blokkeren, data stelen) om daarna losgeld te eisen.

Jorij Abraham van de Global Anti Scam Alliance: 'Ik zou nu eerder van code rood willen spreken. AI is een groot gevaar'

Allereerst een aantal cijfers volgens de politie data: In 2023 waren er 84.861 aangiftes horizontale fraude , waar de meeste gevallen van digitaliseerde criminaliteit onder vallen, in 2022 was dat 83.345, het ophelderingspercentage steeg van 6% naar 8%. Voor cybercrime gold juist een daling van het aantal aangiftes: van 13.996 in 2022 naar 12.029 in 2023. Maar het ophelderingspercentage steeg ook, van 5% naar 6%. Dat percentage geeft aan hoe vaak een aangifte leidt tot een verdachte tegen wie ook de politie ook verder opsporingsmiddelen inzet. Een stijging is dus goed nieuws. Andere methodes zoals de zogenaamde 'stopgesprekken' zijn niet verwerkt in dit percentage. Een 'stop'- gesprek is een goed gesprek met een verdachte, meestal gaat het dan om een tussenpersoon, om hem of haar te bewegen het criminele pad te verlaten.

De politie heeft tien landelijke teams cybercrime en één landelijk team cybercrime. Daarnaast is er één landelijk team gedigitaliseerde criminaliteit, geen specifieke regionale teams. Opsporing wordt verder overgelaten aan de reguliere regionale teams. Politiewoordvoerder Bobby Markus omschrijft het gevecht tegen cybercrime als een wedloop waarbij de politie moet zorgen creatieve criminelen bij te blijven. Daarom wordt er ook veel geïnvesteerd in kennisontwikkeling en verbetering van de methodes. Deze aanpak leidt tot aansprekende successen zoals recent in 2024 bij de aanpak van hacken via " ransomware" zoals LockBit.

In 2023 werd ook gezegd, door bronnen binnen de politie, dat internationale samenwerking en gegevensuitwisseling van groot belang zijn. De cybercrime casus van LockBit lijkt daar een mooi voorbeeld van te zijn.

Toch geeft de politie ook een winstwaarschuwing af. Hiermee is deze vorm van criminaliteit zeker niet definitief een halt toegeroepen. Ook blijft het gissen naar de werkelijk omvang, omdat lang niet alle getroffen bedrijven aangifte doen uit vrees voor wraakmatregelen van criminelen. De politie waarschuwde daarom al in juli 2023 bij het uitbrengen van het Cybersecuritybeeld 2023:

Ransomware is de grootste bedreiging van de digitale veiligheid. Criminelen versleutelen niet alleen computersystemen, maar stelen ook data om andere misdrijven mee te plegen. Dit raakt niet alleen organisaties, maar ook steeds meer burgers. Dat - en meer - blijkt uit het Cybersecuritybeeld Nederland dat vandaag is gepubliceerd.

Het OM zal cijfers over 2022 pas in mei 2024 kunnen publiceren

Het verschil in aanpak tussen die van cybercrime en die van gedigitaliseerde criminaliteit lijkt zich ook te vertalen in de cijfers. Duidelijke daling van het aantal aangiftes voor cybercrime. Lichte stijging van die voor gedigitaliseerde criminaliteit. Regionale teams moeten de aanpak van gedigitaliseerde criminaliteit combineren met veel andere taken, waardoor slachtoffers vaak zien dat hun aangifte geen vervolg krijgt ook al is een potentiële medeverdachte in beeld. Dit werd ook in 2023 al onderkend. De politie probeert wel door voorlichting op verschillende manieren burgers meer bewust te maken van de risico's. Ook zijn er andere methodes zoals de samenwerking die de politie met het platform Marktplaats heeft gezocht.

De conclusie is toch dat burgers voortdurend zelf alert moeten zijn. Vooralsnog wijzen de cijfers – zeker bij gedigitaliseerde criminaliteit – niet op een significante verhoging van awareness.

Andere bronnen, zoals cijfers van de Fraudeheldesk geven een vergelijkbaar beeld met dat van politie. Duidelijke toename van het totaal aantal meldingen, van 51.607 naar 57.580 en lichte toename van de totaal gemelde schade van € 43.221.928,- naar € 44.495.376,- . Er zijn uitzondering zoals afname van de aan- en verkoopfraude, maar daar gaat het meestal om relatief kleine bedragen. Ook hier zijn meldingen (en gemelde schade) m.b.t. cybercrime gedaald.

De grootste gemelde schade wordt blijkens de cijfers van de Fraudehelpdesk veroorzaakt door drie vormen van fraude: dating fraude, beleggingsfraude en voorschotfraude, een exact cijfer van de totale omvang van schade van deze drie categorieën valt niet te geven omdat er overlap zit tussen de drie categorieën. Maar zelfs bij de meest optimistische schatting is wel duidelijk dat deze drie categorieën samen goed zijn voor meer dan de helft van de geleden schade. De Fraudehelpdek zag ook een opvallende toename in pogingen tot oplichting via SMS-jes.

Het Openbaar Ministerie (OM) is verantwoordelijk voor vervolging van door de politie aangebrachte zaken. In 2023 meldde Désirée Wilhelm dat het OM geen cijfers over 2023 kon melden omdat:

De gezamenlijke landelijke aanpak van gedigitaliseerde criminaliteit is pas in ontwikkeling. Het OM vindt het daarom te vroeg om cijfers te delen. Ook omdat de wijze waarop in het heden en toekomst gedigitaliseerde criminaliteit wordt geregistreerd afwijkt van het (recente) verleden. Dit komt omdat het onderwerp sinds dit jaar prioriteit heeft in de Veiligheidsagenda.

Ondanks deze prioriteitstelling zal het OM pas in mei 2024 cijfers over 2022 naar buiten brengen, dit zal gecombineerd worden met cijfers over 2023.

Jorij Abraham van de GASA (Global Anti-Scam Alliance) is er zeker nog niet gerust op. Deze organisatie probeert wereldwijd de vinger aan de pols te houden. Hij spreekt voorlopig van code rood, de mogelijkheden van AI (Artificial Intelligence) en apps zoals chat-GPT worden ook benut door criminelen en dat gaat groeien. Hij denkt dat AI ook benut moet gaan worden om burgers en bedrijven beter te beschermen. Als het gaat om Nederland in vergelijking tot andere landen, dan doet Nederland het overigens zo slecht nog niet bij de preventie en de bestrijding. Voor hem een eyeopener was, dat ook in ontwikkelingslanden zeer veel mensen slachtoffer worden van deze vorm van criminaliteit. Weliswaar gaat het dan om kleinere bedragen, maar die komen door de lagere levensstandaard toch

hard aan. Ook het opnieuw oplichten van eerdere slachtoffers ziet GASA als een trend. Hij stelt zich voor dat in de toekomst telefoons zo beveiligd zijn dat voordat de telefoon overgaat en je op kunt nemen, er al een check op mogelijke oplichting is gedaan.

Vanuit meerdere kanten wordt benadrukt dat burgers en ondernemers zich meer bewust moeten zijn van de risico's, daarom investeert de politie ook veel tijd en moeite in voorlichting en samenwerking met andere partners. Toch moet er meer gebeuren, in de 'position paper' die de politie in mei 2023 uitbracht, wordt gesteld dat voor de aanpak van het thema *Investeren in een digitaal vaardige politie*, een extra investering nodig is, in dit geval van 150 miljoen euro. Dat is gelet op de totale geschatte schade van 25 miljard euro voor deze criminaliteit geen exorbitant hoog bedrag.

René Lesuis

Leesverderr! Publicaties

https://leesverderr.nl

X: https://twitter.com/leesverderr

info@leesverderr.nl