Executive Vice-President of the
EU Commission
Margrethe Vestager (EUROPE FIT FOR A DIGITAL AGE)
margrethe-vestager-contact@ec.europa.eu

Joint Cybercrime Action Taskforce (JCAT)
Europol
P.O. Box 90850
2509 LW The Hague
The Netherlands

Wien, am 14. Juli 2020

Sehr geehrte Frau Vize Präsidentin Vestager !

Betreff:
Unterstützung für die Opfer von Cyberkriminalität!

1. Die European Funds Recovery Initiative (EFRI) wurde 2018 ins Leben gerufen und vertritt inzwischen mehr als 820 Verbraucher, die durch Investment-Betrug um einen kumulierten Verlust von mehr als 34,7 Mio. Euro betrogen wurden.

2. Wie unsere Mitglieder - Opfer von Cyberkriminalität – durch Verlust ihrer Lebensersparnisse lernen mussten, bringt die zunehmende Digitalisierung der Gesellschaft im Allgemeinen und die damit verbundene Virtualisierung des Geldes im Besonderen eine neue, massive Bedrohung für die Verbraucher mit sich: Die transnationale Cyberkriminalität. Die Kombination modernster Technologien mit neuen Marketingmethoden und einer massiven Disparität in der Technikaffinität der Internetnutzer schafft eine noch nie dagewesene Ökosphäre für Kriminelle.

3. Es gibt Tausende europäische Opfer, die wie unsere Mitglieder ihre Lebensersparnisse an international agierende und mafia-ähnlich organisierte Cyberkriminelle auf dieselbe Art und Weise verloren haben.

4. Alle unsere Mitglieder verließen sich in erster Linie auf funktionierende europäische Gerichtsbarkeiten und Strafverfolgungsbehörden. Sie vertrauten auf die Zusagen der europäischen Gesetzgeber, und darauf, dass sowohl die lokalen als auch die europäischen Behörden eine sichere Cyberumgebung sowie einen sicheren Online-Finanzmarkt gewährleisten.

5. Unsere Opfer mussten jedoch leidvoll feststellen, dass, obwohl die Regierungen versuchen, die Digitalisierung voranzutreiben, Bargeld zu eliminieren und die Online-Zahlungsindustrie zu fördern, weder die lokalen Strafverfolgungsbehörden noch die europäischen Vollzugsbehörden wissen, wie man angemessen gegen Cyberkriminalität vorgeht. Modernste Technologie vermischt mit krimineller Energie erfordert eine entsprechende Ausbildung und Erfahrung der Behörden. Zu diesem Zeitpunkt, wo sich die Cybergesellschaft der EU noch am Anfang einer Lernkurve befindet, mussten unsere Opfer mit dem Verlust all ihrer Ersparnisse einen hohen Preis zahlen, um das zu lernen.

6. Wir wenden uns mit diesem Offenen Brief an Sie, um Ihre Aufmerksamkeit auf das derzeit in Wien anhängige Gerichtsverfahren wegen Cyberkriminalität zu lenken, das den mutmaßlichen israelischen Cyberverbrecher Gal Barak betrifft. Für Herrn Barak gilt natürlich die Unschuldsvermutung wie für jeden EU-Bürger auch.

Laufendes Strafverfahren in Wien, Österreich

7. Im Januar 2019 nahmen österreichische Strafverfolgungsbeamte in enger Zusammenarbeit mit ihren EU-Kollegen erstmals Cyberkriminelle fest, die mit ihren Finanzbetrügereien systematisch auf EU-Verbraucher abzielten. Es war mit Sicherheit ein großer Durchbruch im Kampf der EU gegen die Cyberkriminalität.

8. Derzeit findet in Wien der erste EU-Cyberkriminalitätsprozess gegen die festgenommenen mutmaßlichen Betreiber einer ganz Europa umfassenden Cyberkriminalitätsorganisation statt. Wir nehmen diesen Fall daher zum Anlass, Ihre Aufmerksamkeit und die Aufmerksamkeit der Öffentlichkeit auf diesen Wiener Prozess zu lenken.

9. Betrüger, wie der angeklagte Israeli Gal Barak haben ihre Betrügereien über verschiedene Offshore- und Briefkastenfirmen in verschiedenen Gerichtsbarkeiten abgewickelt. Mit ihrer grenzenlosen und länderübergreifenden Vorgangsweise haben sie sich bisher einer strafrechtlichen Verfolgung der Behörden entzogen.

10. Der Prozess gegen Gal Barak kann daher als ein Meilenstein im Kampf gegen die Cyberkriminalität in der gesamten EU betrachtet werden. Einmal mehr gilt die Unschuldsvermutung, aber auch die Verpflichtung des Gerichts, die Wahrheit zu suchen.

Weitere Einzelheiten zum Prozess

11. Die Anklage gegen den Israeli GAL BARAK wurde nach fast zweijährigen Ermittlungen durch die österreichischen Strafverfolgungsbehörden in enger Zusammenarbeit mit Behörden anderer europäischer Länder erhoben.

12. Am 8. Juli 2020 begann in Wien unter Vorsitz des Richters Christian Böhm (LG 122 Hv 4/20g) die Hauptverhandlung im Verfahren gegen den israelischen Staatsbürger Gal Barak.

13. Barak wird von der Staatsanwaltschaft öffentlich des schweren gewerbsmäßigen Betruges sowie der Geldwäsche beschuldigt. Barak ist nur einer von mehr als einem Dutzend Verdächtigen in diesem Strafverfahren, aber aus verfahrensrechtlichen Gründen ist er derzeit der einzige Angeklagte. Er wurde im Februar 2019 aus rechtlichen Gründen aufgrund eines EU-Haftbefehls in Bulgarien verhaftet, wo er zusammen mit seiner Frau Marina Barak (ehemals Marina Andreeva) die Firma E&G Bulgaria EOOD in Sofia leitete.

14. Gal Barak war, zusammen mit seinen Partnern, dem Russen Vlad Smirnow und dem Israeli Gary "Gabi" Shalon, der wirtschaftliche Eigentümer von betrügerischen Online-Tradingwebseiten wie XTraderFX, SafeMarkets, OptionStarsGlobal, Golden Markets oder CryptoPoint. Zusammen mit seiner Frau, der bulgarischen Staatsbürgerin Marina Barak, war Barak nicht nur für die Verwaltung der illegalen Boiler Rooms (Call-Center) in Bulgarien, Serbien und Montenegro, sondern auch für die Geldwäsche der Gelder zuständig. Er errichtete ein die ganze Welt umspannendes illegales Finanzsystemnetz unter Verwendung zahlloser Mantelgesellschaften und illegaler, aber auch lizenzierter Zahlungsabwickler wie Payvision und Wirecard.

Betrug mit Online-Trading-Websites

15. Betrügereien auf Online-Handels-Websites (auch bekannt als Investmentbetrug oder Broker-Betrug) haben mit zunehmender Digitalisierung, insbesondere in Europa, exponentiell immens zugenommen. Schätzungen sprechen von Verlusten von bis zu 12 Milliarden Euro pro Jahr.

16. Die Herangehensweise an diese Art von Online-Betrug lässt sich auf der Grundlage der Aussagen in der Anklageschrift gegen Gal Barak auch wie folgt zusammenfassen

- Die Opfer werden entweder durch Werbung in sozialen Medien oder durch Anrufe von Boiler-Room-Agenten angeworben
- Die Call-Center-Mitarbeiter präsentieren sich als hochprofessionell erfahrene Wertpapierhändler und geben falsche Identitäten und/oder Referenzen an. Häufig wissen sie jedoch bereits über die persönlichen und finanziellen Verhältnisse des potentiellen Opfers Bescheid, da diese Daten zugekauft wurden. Diese Boiler Room-Agenten sind im Vorfeld psychologisch geschult und arbeiten nach genauen Anweisungen oder Skripten, die von Soziologen und Psychologen entwickelt wurden.
- Nach den ersten kleinen Einzahlungen wird den Opfern mündlich, aber auch visuell suggeriert, dass es für sie möglich ist, gewinnbringend in binäre Optionen, Forex oder Kryptowährungen zu investieren, indem sie die Guthaben auf ihren Online-Konten erhöhen.
- Durch tägliche Telefongespräche, professionelles Auftreten und geschicktes Anfordern von mehr persönlichen Daten wird eine enge persönliche Beziehung zwischen dem Boiler Room-Mitarbeiter und dem Opfer hergestellt und damit ein Vertrauensverhältnis aufgebaut, das dazu führt, dass der Kunde noch mehr Geld einzahlt.
- Es kommt jedoch nie zu Auszahlungen der angeblich hohen Gewinne. Nach einer Weile wird den Opfern mitgeteilt, dass das ganze Geld einfach verloren ist.

.

17. Basierend auf dieser Vertrauensbildung wurden Zehntausende von Kunden in Europa von Baraks Boiler Room-Agenten überzeugt, mehr als 200 Millionen Euro über einen Gesamtzeitraum von 2 Jahren einzuzahlen.

18. Tatsächlich wurde das von den Kunden eingezahlte Geld nie für die Veranlagung mit Finanzinstrumenten verwendet, sondern zu 75 % an die beteiligten Dienstleister (Boiler Room-Mitarbeiter, Softwareanbieter, Marketing-Dienstleister, Werbedienstleister usw...) ausgezahlt, und die restlichen 25 % der Einzahlungen der Opfer wurden von den Betrügern zur Finanzierung des luxuriösen und teuren Lebensstils der Betrüger verwendet.

19. Sobald die Opfer ihr Geld verloren hatten, mussten (und müssen) sie erfahren, dass die Strafverfolgungsbehörden und Gerichte nicht in der Lage sind, ihnen zu helfen. Sie mussten die Probleme, Einschränkungen und die Unfähigkeit der europäischen Strafverfolgungsbehörden und Gerichte im Zusammenhang mit Cyberkriminalität erkennen. Offensichtlich ist die Strafverfolgung zur Bekämpfung der Cyberkriminalität auf nationale Grenzen beschränkt und durch diese eingeschränkt, während Cyberkriminelle keine Grenzen kennen und ihnen scheinbar auch keine Grenzen gesetzt werden.

Die Opfer sind einfach nur dumm und lieben den Nervenkitzel !

20. Es ist die Pflicht und verfassungsmäßige Verpflichtung eines Strafverteidigers, alle gesetzlich zulässigen Mittel einzusetzen, um seine Mandanten vor einer Verurteilung zu schützen. Er darf jedoch weder die Opfer kriminalisieren noch andere gegen sein besseres Wissen und Beweismaterial beschuldigen.

21. Gal Baraks Verteidiger, Dr. Peter Lewisch - Partner einer der teuersten Kanzleien Wiens - betonte in seinem Eröffnungsplädoyer vom 8. Juli 2020 erwartungsgemäß die Unschuld seines Mandanten, der sich im Übrigen als vermögenslos ausgibt. Tatsächlich seien die Opfer selbst schuld, erklärte Lewisch in seinem Plädoyer. Nur "dumme" Leute würden den Anzeigen in den sozialen Medien oder den Versprechungen der Boiler Room-Agenten glauben, und dabei sei es irrelevant, dass sie Künstlernamen verwenden, da die "dummen" Leute alles glauben würden.

22. Lewisch führte weiter aus, dass es eigentlich nicht um Investitionen oder Online-Handel gehe, sondern um Wetten, d.h. um ein lotterieähnliches Glücksspiel. "Die Leute lieben den Nervenkitzel, deshalb würden sie so etwas tun", so Lewisch weiter.

Unsere Bitte an Sie:

23. Wenn man die Aussagen dieses Anwalts als Staat oder Gericht akzeptiert, kann der Weg in eine Cyber- oder bargeldlose Gesellschaft nicht beschritten werden. Denn dann würde jeder Betrug an einem Verbraucher indirekt dem Verbraucher selbst angelastet werden. Wie können wir dann von den Bürgern erwarten, dass sie bargeldlos leben, online einkaufen oder Online-Banking betreiben?

24. Leider wird die Cyberkriminalität im Verbraucherbereich oft noch als Bagatelldelikt betrachtet. Tatsächlich gefährdet die Cyberkriminalität die digitale Zivilgesellschaft und ihre Grundwerte, da die Menschen ihre Ersparnisse verlieren und gezwungen sind, sich der Altersarmut zu stellen.

25. Wir sind überzeugt, dass es in der Verantwortung von Staaten, Gerichten und Strafverfolgungsbehörden liegt, diese Art der Cyberkriminalität mit allen ihnen zur Verfügung stehenden Mitteln zu bekämpfen. Es darf in dieser Hinsicht keine Toleranz geben.

26. Dies vorausgeschickt, sind wir der Meinung, dass die Verfahren im Bereich der Cyberkriminalität in den einzelnen Ländern von der EU aufmerksam verfolgt und überwacht werden sollten, um Erfahrungen zu sammeln und diese in Zukunft in Form von Richtlinien oder Initiativen im Kampf gegen die Cyberkriminalität umzusetzen.

27. Das Prinzip, das Opfer zum Täter oder Komplizen zu machen, kennen wir aus dem Gesetz über Sexualdelikte. Bis vor kurzem wurden Opfer von Vergewaltigung, Nötigung oder sexueller Belästigung zumindest als Mittäter dargestellt. Erst die jüngsten Reformen des Strafrechts haben begonnen, die Diskriminierung zu beseitigen. Nun scheint es, dass auch die Opfer von Finanztransaktionen diesen Weg einschlagen müssen. Zumindest versucht Dr. Peter Lewisch, diesen Weg der Diskriminierung des Opfers einzuschlagen, um seinen Klienten vor einer Verurteilung zu bewahren.

28. So wenig die Opfer von Sexualstraftätern die Vergewaltigung, Nötigung oder Belästigung oder den Nervenkitzel suchten, so wenig suchten die Opfer von Betrügern nicht den Verlust Ihrer Lebensersparnisse. Gemessen an der strengsten Definition des Strafrechts jeder EU-Jurisdiktion wurden sie belogen und getäuscht. Die Opfer waren so vertrauensvoll, wie sie nur sein konnten - und wurden betrogen.

29. EFRI wird ihr Bestes tun, um den Opfern von Betrug und Cyberkriminalität eine starke Stimme zu geben, um sie davor zu schützen, vor den Gerichten erneut diskriminiert und schikaniert zu werden. Wir sind der Meinung, dass vertrauensvolle Konsumenten momentan, auf sich allein gestellt sind und dieser grenzenlosen Cyberkriminalität in Europa hilflos ausgeliefert sind Sie haben wenig bis gar keine Hoffnung, dass der Gerechtigkeit endlich Genüge getan wird. Es ist an der Zeit, sich um diese Opfer zu kümmern und die Cyberkriminellen davon abzuhalten, vertrauensvolle Europäer abzuzocken und sie in der Folge auch noch zu beschämen.

30. Wir sind der Meinung, dass es an der Zeit ist, dass die europäischen Behörden Verantwortung für die vor sich gehende Cyberkriminalität übernehmen und sich uns in unserem Kampf gegen die Cyberkriminellen anschließen und uns unterstützen.

Mit freundlichen Grüßen

Elfriede Sixt Nigel Kimberly