**„STOP Dezinformacji – część druga”**

**Transkrypcja podcastu**

[00:00:00 Karolina Małagocka] Policja sobie dość dobrze radzi z działaniami w cyberprzestrzeni. Ciężko mi jest powiedzieć, jaka jest różnica między „off” i „on”, i czy na pewno jesteśmy kiedykolwiek „offline”, bo właściwie cały czas jesteśmy „online”. Niestety ta technologia trochę idzie w kierunku dawania oczu i uszu coraz większej ilości przedmiotów. My możemy stać się jakby źródłem tworzenia „deep fakeów”. Naszą przyszłością niestety mogą być „hejterskie fake newsy”.

[00:00:35 Patrycja Długoń] Patrycja Długoń, witam serdecznie i zapraszam na drugą część rozmowy z doktor Karoliną Małagocką z Akademii Leona Koźmińskiego w Warszawie. Pierwsza część, do której wysłuchania gorąco zachęcam, kończyła się radą naszej ekspertki, aby informacje o świecie czerpać jednak z portali informacyjnych, a media społecznościowe -by służyły kontaktom z osobami, które znamy, i do których mamy zaufanie. W drugiej części policyjnego podcastu nadal rozmawiamy o dezinformacji. Nadmieniłam, że według badań, aż 95% dystrybucji fałszywych informacji o wojnie w Ukrainie - ma miejsce w oparciu o kanały antycovidowe. Czy to ci sami ludzie? Te same narzędzia?

[00:01:22 Karolina Małagocka] Ten sam mechanizm. W cyberbezpieczeństwie się mówi, że nie ma tego zjawiska, że pomarańczowe to nowy czarny, bo nie mamy nowego czarnego. To znaczy te same mechanizmy zdają się sprawdzać od lat, i tutaj, w przypadku dystrybucji różnych treści dezinformacyjnych, jeżeli komuś się udało przejąć konta…. Bo jeżeli chodzi o tożsamość w Internecie - możemy komuś ukraść tożsamość, i to jest akurat obłożone nawet w Polsce już karą, zgodnie z Kodeksem Karnym do 3 lat, czyli nie mogę po prostu bezkarnie przejąć czyjeś tożsamości i się nią posługiwać w Internecie. Ale jest dużo ciężej z przejęciem konta. To znaczy, dużo ciężej jest udowodnić, że ktoś przejął czyjeś konto zwłaszcza, jeśli to przyjęcie nie nastąpiło z terytorium Rzeczypospolitej. No i ofiara też niekoniecznie musi sobie w ogóle zdawać sprawę, a nawet jak sobie zdaje sprawę, to jest to trudne do udowodnienia. Więc te konta są przyjmowane dlatego, że wyciekają nasze dane do Internetu. Niektórzy mówią, że nawet do 500 rekordów na sekundę wycieka. Czyli znamy czyjeś hasło, znamy login, znamy inne dane osobowe, z których oczywiście „boty” mogą próbować tworzyć hasła - te, którymi się posługujemy w mediach społecznościowych. W ten sposób następują przyjęcia kont, no i teraz te konta są przejęte, albo są celowo tworzone, łączone ze sobą w całe farmy, no i tak są rozprzestrzeniane informacje. Jeżeli sprawdzało się to w przypadku Covidu, no to potem możemy też równie dobrze wykorzystać te same kanały do rozprzestrzeniania informacji o wojnie w Ukrainie. Tyle od strony dystrybucji. Od strony odbiorców, jeżeli ktoś ma ogólną tendencję do wiary w to, że dociera do informacji „tajnych przez poufne” - możemy je sobie tak nazwać - albo takich, które są ekskluzywne, bo nikt wcześniej o nich nie przeczytał, to prawdopodobnie ta jego tendencja nie znikła. To znaczy, tak było w przypadku Covidu, tak będzie w przypadku wojny w Ukrainie, i to znowu będzie bazowało na podkręcaniu tych złych emocji.

Jeżeli ktoś faktycznie ma w sobie złość na istniejącą sytuację… Możemy powiedzieć, że wszyscy mamy tą złość, ale jeśli ktoś tą złość jeszcze w sobie kultywuje, właśnie doczytywaniem informacji, do których inni nie mają dostępu - to to będzie osoba, która się tak zachowuje. Te modele behawioralne są w ten sposób też tworzone, w związku z tym wiadomo, że ona będzie dobrą osobą do tego, żeby jej przekazywać, i dalej będzie przekazywała. To są właśnie pewnie potem te niekończące się dyskusje przy stołach rodzinnych, gdzie mamy… - prawdopodobnie, każdy z nas ma w swoim najbliższym otoczeniu chociaż jedną taką osobę, która wchodzi i zaczyna od tego: „A słyszeliście? Bo ja przeczytałem/przeczytałam...”. I to tak też się dzieje w sieci, to znaczy ta jedna osoba, która jest święcie przekonana, że ten świat tak wygląda, jest tak zbudowany - jest w stanie informować bardzo dużo innych, i siać ten element ewentualnego, chociaż zapytania: „A może coś w tym jest?”. Tak, „chociaż ziarenko prawdy?”. To ziarenko prawdy jest dla nas bardzo zwodnicze, bo ono potem kiełkuje właśnie w różne takie niestworzone, czasem ciężkie do wykorzenienia teorie.

[00:04:33 Patrycja Długoń] Jak na nas działają informacje, które nie są prawdziwe? Jak na nas działa dezinformacja?

[00:04:38 Karolina Małagocka] Zawsze się mówiło, że kłamstwo jest bardziej atrakcyjne od prawdy. To znaczy, to jest dobrze widać w nauce - jak mamy badania naukowe, to one są zasadniczo nudne, i właśnie dlatego zdarza się naukowcom… I tutaj chyba Covid jest świetnym przykładem - przedstawiać swoje badania rzetelnie, wyniki rzetelnie, ale potem mamy tą część, w której piszemy wnioski… Nam się zdarza wtedy tworzyć takie wnioski, które są bombastyczne, a dokładnie tak było z Amantadyną. To znaczy, tam było 14 pacjentów, których przebadano, faktycznie okazało się, że istnieje jakiś związek pomiędzy Amantadyną a blokowaniem białka, i to był koniec badania. I ono było nieciekawe. Więc napisano, że Amantadyna potencjalnie leczy Covid, co bezpośrednio z tego badania nie wynikało, i oczywiście autorzy tego artykułu się wycofali. Zostali zmuszeni do poprawienia tego artykułu i do poprawienia tych wniosków. Więc tak jest… To znaczy, jak ja bym dzisiaj prezentowała swoje wyniki badań naukowych, to mam tam jakąś grupę, z tego są jakieś wnioski, i one są na ogół mało spektakularne, ale oczywiście jak ja je zaczynam uogólniać na całe społeczeństwo, no to mogę sobie tworzyć bardzo fantastyczne teorie. Więc czasem też tak jest, że bierzemy coś, co ma źródło naukowe, i faktycznie ktoś gdzieś jakieś badania przeprowadził, tylko po prostu wnioski, które z tego są wysnuwane i przypisywane badaniom naukowym, są zupełnie niewspółmierne do tego, co zostało zbadane. I dlatego tak łatwo jest nam uwierzyć w różnego rodzaju dezinformacje. To znaczy ciężko jest nam uwierzyć, że przez 10 godzin działań wojennych, nie zmarł ani jeden cywil. Zdecydowanie lepiej jest nam uwierzyć, że pod gruzami szpitala 170 kobiet straciło życie, i to jest ta informacja, która się jakoś wpisuje w nasz zły obraz wojny. Poza tym nie jest newsem, i dlatego też na przykład nie aktualizują się strony informacyjne, bo jeżeli nikt nie zginął no to nie ma o czym informować. Stara zasada dziennikarska: „lead must bleed”, czyli że musi nam krwawić ten tytuł, żeby ludzie chcieli go klikać. Niestety jesteśmy też do tego coraz bardziej przyzwyczajeni, więc my trochę włączamy te media z takim oczekiwaniem, że ktoś nam powie o czymś szokującym. Jeżeli tych szokujących informacji nie ma, a pojawiają się gdzie indziej, no to zaspokaja naszą potrzebę.

[00:06:58 Patrycja Długoń] Czasami zdarza się, że przechodzimy do działania i robimy coś, co jest wynikiem przejmowania tego sztucznego obrazu rzeczywistości…

[00:07:10 Karolina Małagocka] No tak, wszystkie paniki konsumenckie, które ostatnio miały miejsce, to jest właśnie taki chyba naoczny efekt tego, że można ludzi faktycznie skłonić do podejmowania działań, których prawdopodobnie by się nie podjęli.

[00:07:22 Patrycja Długoń] Podpalenie w Wielkiej Brytanii masztów 5G, albo niedawno pobicie przez czterech sprawców trzech uchodźców w Przemyślu…

[00:07:33 Karolina Małagocka] I to jest właśnie chyba największe zagrożenie, bo o ile kupowanie papieru toaletowego możemy powiedzieć, że było zabawne (może dla niektórych stanowiło swoiste wyzwanie), i dzisiaj się z tego możemy śmiać, to ciężko się śmiać z pobicia, albo z podpaleń, albo z innych aktów przemocy. Ja zawsze mówię, że dopóki jeszcze rozmawiamy o jakiś zachowaniach konsumenckich, takich szeroko rozumianych, że ktoś coś będzie kupował, albo nie kupował, to jeszcze jest naprawdę niewielki problem. Dużo gorzej, jak wchodzimy w tą sferę racji czysto takich międzyludzkich, a to działają te same mechanizmy, to znaczy te osoby, które najpierw zostały namówione do tego, żeby kupować papier, kupować paliwo, nie wiem… kwestionować sensowność szczepień albo noszenie maseczek, czyli też wpływały już wtedy na poziom naszego zabezpieczenia zdrowotnego... z tej ogromnej masy ludzi, bo przecież rozmawiamy o tysiącach użytkowników - naprawdę mogą znaleźć się tacy, którzy niestety odpowiedzą czynem na wezwanie, że uchodźcy stanowią źródło jakiś potencjalnych problemów, i trzeba ich stąd wyrzucić. Albo chociaż zachęcić ich aktywnie do wyjazdu. Więc to nie jest tak, że nagle wszyscy ci sami ludzie, którzy kupowali papier, zwrócą się siłowo przeciwko powiedzmy uchodźcom. No, ale wystarczy nam niewielki procent, tak jak mówiłam, to dotyczy tysięcy ludzi, więc w tych tysiącach ludzi prawdopodobnie znajdzie się ktoś, w kim już jest ten element agresji, i odpowiednio pobudzony - przystąpi do działania. I to jest nasz największy problem, bo nigdy nie wiemy, jak dużo tych ludzi będzie, i czy my będziemy w stanie ich odpowiednio wcześniej wyłapać, albo czy będziemy mieli tyle sił, chociażby, porządkowych, żeby zapobiec jakimś większym zorganizowanym działaniom. Chciałam zwrócić uwagę, że mamy takie zjawisko platformizacji i mówi się o deplatformizacji - to jest w przypadku wszystkich tych ruchów, zwłaszcza w Stanach Zjednoczonych, ale też mówiło się o Państwie Islamskim. Ponieważ staraliśmy się wyrzucić tych spiskowców, „człowieka bizona”, który wszedł na Kapitol, tak? I jego kolegów i koleżanki z oficjalnych platform z mediów społecznościowych - usuwano ich konta, tak samo jak czyniono to z, oczywiście, Al-kaidą i poplecznikami. Więc oni zaczęli tworzyć własne platformy. I to nie jest tak, że tego nie będzie nigdy w Polsce, to znaczy już mamy całą masę osób, które organizują się w platformy, i widzimy, że to jest duży problem. Bo oni na tych platformach, które już wtedy pozostają poza oficjalnym obiegiem - wymieniają się nie tylko niestety tymi niestworzonymi informacjami i teoriami, ale też potrafią się organizować w bardzo agresywne ruchy. Obecnie mamy przykład od nas bardzo daleki, taki… niekoniecznie się nim interesujemy, czyli kierowców ciężarówek w Kanadzie, którzy blokują miasta. Właśnie nie podobają im się Covid i to, co się dzieje z Covidem, więc my oczywiście się tym nie interesujemy, mamy własne problemy, ale jestem w stanie sobie wyobrazić… No, w Polsce chyba dobrym przykładem są ruchy kibolskie - czyli nie kibiców, ale kiboli, którzy przecież też właśnie zaczynają się organizować w Internecie, w Darknecie, ale też w takich miejscach, które pomału zaczynają nam przypominać nieformalne platformy. Wydaje mi się, że to będzie przyszłość - walka z tego typu zjawiskami.

[00:10:52 Patrycja Długoń] No właśnie, Policja jest na tej pierwszej linii. Na co Pani zdaniem powinniśmy zwrócić szczególną uwagę, jako Policja?

[00:11:03 Karolina Małagocka] Na dziś myślę, że na wszystkie sygnały, które nie tylko mówią właśnie o tym, żeby coś kupować, albo nie kupować, ale te, które mówią o fizycznym zagrożeniu. Czyli, że jesteśmy fizycznie zagrożeni ze strony kogoś, bo to może się bardzo łatwo przełożyć na fizyczną agresję. Myślę, że przyszłość działań… Zresztą Policja sobie dość dobrze radzi z działaniami w cyberprzestrzeni, bo tak jest. Nawet ta dyskusja, czy zgłaszać „fake newsy” na Policję? Do kogo na Policji? - to, to pokazuje, że jednak mamy tą wiarę, że Policja jest w stanie coś w cyberprzestrzeni zrobić. Myślę, że tutaj siły zasłużyły sobie szczególnie działaniami w obszarze ochrony dzieci, i całą tą walką z pedofilią dziecięcą. Wszyscy mieliśmy okazję usłyszeć o sukcesach na tym polu, i to jest bardzo ważne. Myślę, że kolejnym ważnym wyzwaniem będzie właśnie wynajdywanie tych miejsc w Internecie, gdzie takie osoby się gromadzą, i gdzie faktycznie następuje to przejście od czystego teoretyzowania, do tego, że faktycznie coś jest problemem, czyli do organizowania się już w fizyczną przemoc. Bo nie ma chyba nikt dziś wątpliwości, że to już nie polega na tym, że kolega namówił kolegę, czy koleżanka koleżankę, tylko niestety to są często zupełnie obce osoby, które po prostu się organizują w sieci. I sprawne, nie tylko wynajdywanie tych miejsc, ich monitorowanie, bo wierzę, że to Policja dzisiaj robi - no, ale też to, do czego teraz coraz częściej wzywamy, czyli do deplatformizacji tych ruchów. To będzie przyszłość walki z tego typu zagrożeniami. Zagrożeniami, które często będą zupełnie abstrakcyjne, to znaczy ktoś rzuci hasło, że musimy zlikwidować całe, powiedzmy… osiedla uchodźców, bo tam jest coś złego. I to może być dowolna abstrakcyjna przyczyna. Więc myślę, że dzisiaj trzeba być szczególnie wyczulonym na to, co się w tej sieci pojawia, i gdzie te informacje się pojawiają, a także, dokąd ci ludzie potem trafiają. Bo to, że oni są na Facebook, to że oni są na Twisterze - to jest jedno pytanie, ponieważ Facebook i Twitter prawdopodobnie już bardzo szybko poradzą sobie z likwidacją tego typu skupisk. Natomiast gdzie oni dalej trafią, to będzie wielkie wyzwanie, które właściwie czeka już za rogiem.

[00:13:17 Patrycja Długoń] Mówi pani samozwańcach, co to jest za grupa?

[00:13:20 Karolina Małagocka] Na przykład dzisiaj mamy taki ogólny zachwyt nad tym, co robi grupa Anonymus. I ciężko powiedzieć, że nam się to nie podoba. No bo to, co oni robią - się wpisuje w naszą koncepcję walki z rosyjską propagandą, czyli sami nic nie możemy zrobić, no bo jesteśmy od nich daleko, no ale są jacyś ludzie, którzy faktycznie robią to w naszym imieniu, i nam się to podoba. Ja bym tu była trochę daleka od takiego całkowitego bezkrytycznego zachwytu. To znaczy, po pierwsze: warto zwrócić uwagę, że jeżeli ktoś jest specjalistą od IT, to niekoniecznie musi być specjalistą od polityki międzynarodowej, i prawdopodobnie nie jest. Po drugie: no my nie wiemy, kto to jest, a wymyśliliśmy sobie zasady i chcemy przestrzegać prawa, które ustalamy dla wszystkich. Oni jawnie tego nie robią, czyli jawnie je łamią. Po pierwsze, mają środki i zasoby, żeby je łamać. Po drugie, dzisiaj je łamią i nam się to podoba, jutro będą je łamali i nam się może nie podobać. No i po trzecie, wiadomo, że najłatwiej jest złamać system, który się dobrze zna, więc warto zadać sobie pytanie: kto to jest tak naprawdę? I czy każdy z nas, gdyby nam tak otworzyć dostęp do zasobów rosyjskich służb specjalnych, umiałby tam znaleźć dane szpiegów? Ja bym nie umiała osobiście, tak? To znaczy, nic nie wiem o działaniu służb specjalnych poza tym, co mogę wyczytać w Internecie, w legalnych źródłach, więc nie umiałabym stwierdzić, kto jest oznaczony, jako szpieg. To znaczy, po prostu bym tego nie wiedziała. Pytanie zatem: kto to robi? Kto ich finansuje? I w czyim imieniu oni działają? I co jeszcze mogą zrobić? Plus taka rzecz, która mnie osobiście najbardziej przeraża, to znaczy… Oni działają w naszym imieniu. Nie mamy na nimi żadnej kontroli, no i mogą sobie wybrać jakiś ruch, który Rosja by odczytała, jako ruch wojenny, no i wtedy oczywiście odpowiedź byłaby raczej skierowana nie w stronę Anonymus, tylko w stronę nas, fizycznie. I to jest duże zagrożenie, no i możemy sobie wyobrazić, że takich ruchów będzie więcej. Anonymus żyją od 2010, jeśli się nie mylę, i od wtedy różne działania przeprowadzają. Wydaje mi się, że spojrzenie na hakera takie, które wytworzyły nam filmy… jeszcze w 95 roku „Hakerzy” z Angeliną Jolie…. Angelina Jolie wygląda tam jak nie dzisiejsza Angelina Jolie, i zapewniam Państwa, że hakerzy, o których wtedy była mowa, którzy zostali nam w głowie, czyli tacy super inteligentni, super utalentowani ludzie w bluzach, działający jako samotne wilki…. I tak samo, jak Angelina Jolie dziś wygląda inaczej, hakerzy też dzisiaj wyglądają inaczej. To są na ogół bardzo dobrze zorganizowane grupy, dobrze dofinansowane, często gęsto związane z działaniami rządów. Nie wiemy których rządów i nie wiemy których grup. No, ale możemy się spodziewać, że takich samozwańców będzie coraz więcej, i tutaj widzę dwa zagrożenia, o których się już dzisiaj mówi. Po pierwsze, o wciąganiu młodych ludzi, zdolnych ludzi w działania przestępcze. I to warto sobie zwrócić uwagę, że to zawsze są działania przestępcze, nawet jeśli dzisiaj mówimy, że one nam się jakoś podobają. Wydaje mi się, że gloryfikacja tych działań jest trochę ryzykowna na przyszłość. No a po drugie, jednak… że te nasze zasady mogą być łamane, no i pytanie: kto i w czyim imieniu to robi? - też będzie bardzo ważne. Walka z tymi dużymi grupami, dobrze dofinansowanymi i świetnie wyszkolonymi, będzie prawdopodobnie też dużym wyzwaniem, no a my nie wiemy kogo następnego, i jaki cel sobie obiorą, a więc warto to rozpatrywać przynajmniej w tych dwóch aspektach, tak? Czyli, że nie mamy nad nimi kontroli, i oni łamią jawnie prawo, i potrafią to robić skutecznie. No i drugie, że zaczyna być to bardzo akcyjne, więc możemy się spodziewać, że teraz ileś tam młodych osób, prawdopodobnie również w Polsce siedzących, myśli sobie o tym, że mogłoby dołączyć do takiego ruchu, no a na koniec będziemy musieli sobie prosto w twarz powiedzieć, że to są ludzie, którzy złamali prawo.

[00:17:13 Patrycja Długoń] Ale współpracuje Pani z etycznymi hakerami. Proszę powiedzieć w takim razie, czym się oni charakteryzują, i na jakim polu Pani z nimi współpracuje.

[00:17:25 Karolina Małagocka] Mówimy o ludziach, którzy są „white hat hackers” i „black hat hackers”, tak? Czyli biała - czarna czapka. Trochę chodzi o to, tak? To znaczy, to są te same narzędzia. Tutaj to nie jest tak, że my mamy jakieś inne narzędzia, które wykorzystujemy, żeby zabezpieczać systemy informatyczne. Na ogół my mamy tą samą wiedzę, i ci ludzie kończyli prawdopodobnie te same szkoły. To, co my robimy, to staramy się być o krok przed nimi, czyli faktycznie tworzyć takie rodzaje zabezpieczenia, i na tyle edukować użytkowników, żeby włamywanie się do tych systemów było coraz trudniejsze, żeby wymagało też coraz więcej zasobów, bo nie oszukujmy się - każdy system, co człowiek wymyślił, drugi człowiek jest w stanie złamać. Więc jest to prawdopodobnie tylko kwestia stopnia trudności, ilości zasobów, które trzeba zaangażować. To też dlatego doradzam, żeby zabezpieczać swoje urządzenia nawet, jeśli ktoś żywi przekonanie, że nigdy nie widział żadnego zagrożenia internetowego, i go nie spotka tego typu problem, bo nie jesteśmy najniżej wiszącym owocem. Czyli, jeżeli ktoś ma się włamać do jakiegoś urządzenia (na ogół robią to boty, które sobie krążą po Internecie, szukają po prostu tego miejsca, gdzie się jest najłatwiej włamać), no to może się nam zdarzyć, że to po prostu za którymś razem będzie nasza komórka, czy nasz komputer, albo nasza firma. Dlatego też ci etyczni hakerzy, tak? To jest chyba te określenie, którego też lubimy używać, to są ci, którzy myślą o tym, jak najlepiej się zabezpieczyć w Internecie, i jak nie dopuszczać do tego, żeby łamanie tych zabezpieczeń było łatwe albo tanie. No, bo to trzeba powiedzieć, że to jedno i drugie ze sobą… ma dużo wspólnego, a że takie działania są podejmowane, i są one wysoko nieetyczne, bo to też można sobie powiedzieć… No dobrze, jeśli chodzi o pieniądze, to gdzie tutaj ta etyka. Jak zaczęła się pandemia Covidu, najczęściej atakowanymi instytucjami były szpitale i punkty testowania. Tam stosowano metodę „ransom ware”. „Ransom” - okup, „ware” od oprogramowania, czyli po prostu blokowano dostęp do zasobów całych sieciowych, w zamian za zapłacenie określonej kwoty. To się wydarzyło na przykład w Czechach. W Brnie już trzeciego dnia oficjalnej pandemii jedyna stacja testowania w Czechach została w ten sposób zamknięta. Nie wiemy do końca jak się skończyło, bo ona dość szybko wróciła do pełnego działania. Oczywiście tutaj jakby oficjalne informacje były takie, że po prostu udało się ją przywrócić.

[00:19:58 Patrycja Długoń] A ja słyszałam o tym, że odwołano operacje i jednak tam się zadziało…

[00:20:03 Karolina Małagocka] Tydzień czasu to trwało. Prawdopodobnie, nie wiemy tego. Tak wiemy, że są instytucje, które płacą, są instytucje, które absolutnie nie płacą, i w tym momencie muszą postawić jakby część, przynajmniej, systemu od nowa. No, ale to pokazuje jak nieetyczne mogą te działania być. Bity i bajty nie mają czerwonego krzyża, ani czerwonego półksiężyca. Nie dorobiliśmy się tego, czyli właściwie ci sami ludzie, którzy dzisiaj mają potencjał atakowania stron rosyjskich, warto to sobie gdzieś tam odnotować, mogliby potencjalnie zaatakować dowolną inną instytucje. W związku z tym… Dlatego te działania, które polegają jednak na atakowaniu, no… musimy określać, jako nieetyczne. Nawet jeśli wpisują się w nasz obraz dzisiejszego świata.

[00:20:52 Patrycja Długoń] Wracając do samej dezinformacji, również ona jest wykorzystywana do zdobywania danych wrażliwych - w jaki sposób?

[00:21:00 Karolina Małagocka] No na przykład, jeżeli dostajemy informację, która jest do nas dobrze dopasowana, więc powiedzmy jakoś tam spersonalizowana, pochodzi teoretycznie od źródła, od którego moglibyśmy dostać informację - na przykład naszego operatora Internetu, dostawcy gazu, prądu, no…. I tam pojawia się prośba o kliknięcie właśnie w link, albo o zalogowanie się. To są wszystko te miejsca, gdzie potencjalnie niekoniecznie musi chodzić o kradzież pieniędzy, a kradzież pieniędzy z konta bankowego wymaga dużo zachodu. Trzeba umieć to zrobić, trzeba mieć na to odpowiednie środki, i potencjalnie jeszcze narażamy się na to, że tą sprawą mogą się zainteresować organy ścigania. Więc to jest duża sprawa. Wykradanie informacji takich prywatnych, jest dużo łatwiejsze, a też można je sprzedać. Po pierwsze, można je sprzedać w Internecie, po drugie - dużo łatwiej się to robi, no i jesteśmy mniej narażeni na to, że ktoś będzie nas na koniec dnia ścigał. A jeżeli wykradamy informacje o użytkowniku, no to mamy kolejne możliwości ataku coraz bardziej zaawansowanego, coraz lepiej dopasowanego. Więc jak najbardziej wiemy też coraz więcej o tej osobie, więc właśnie możemy spróbować przyjąć jej konto. Kiedyś do tych przyjęć kont masowo dochodziło przed wyborami. Myśmy widzieli, że konta był przyjmowane na przykład w Polsce przed wyborami, istotnymi wyborami, na przykład przed samorządowymi mniej, ale już przed parlamentarnymi, prezydenckimi - to był zdecydowany pik w tych przejęciach kont. Więc tutaj jak najbardziej tego typu działania się ze sobą łączą. Warto dzisiaj zwrócić uwagę, że tych danych wyciekają ogromne ilości. Nie zawsze ze względu na atak, czasem nam wyciekają, bo ktoś ich nie dopilnował, i one po prostu mogły zostać przejęte. Dlatego też w naszym rozporządzeniu o ochronie danych osobowych, mamy ten artykuł 32, który nakłada na firmę obowiązek zabezpieczenia systemów informatycznych, no chociażby po to, żeby ograniczyć ten wyciek danych. Ponieważ zawsze ofiarą jest końcowy użytkownik, każdy z nas, bo my tych danych nie możemy już wymazać, a one o nas są i krążą. Więc jak najbardziej warto zwracać uwagę na to, gdzie się te swoje dane zostawia, ale też komu się jej powierza, czy korzystanie z różnego rodzaju niesprawdzonych oprogramowań, które są pobierane poza oficjalnym sklepem, ewentualnie wypełnianie formularzy wszelkimi możliwymi prawdziwymi informacjami - to się warto zawsze zastanowić, czy muszę podać prawdziwe informacje. Naprawdę, ja proponuję się zastanowić, i mieć przynajmniej kilka adresów mailowych, którymi się posługujemy. Jeśli nie, to takie chwilowe adresy mailowe. Przynajmniej kilka adresów mailowych. I wszędzie tam, gdzie naprawdę niepotrzebna jest informacja o tym, jak mamy na imię, nazwisko, albo kiedy się urodziliśmy…. Warto na to zwrócić uwagę. Warto zwrócić też uwagę, że każda informacja jest informacją wrażliwą. Żeby w ogóle warto porzucić myślenie o tym, że są jakieś informacje niewrażliwe, bo drugie imię jest w Polsce takim dobrym przykładem. Dużo łatwiej zidentyfikować osobę, nawet jeśli szukamy tylko o tej osobie informacji - jeżeli znamy jej drugie imię. To bardzo zawęża i zwiększa możliwości wyszukiwania. Jeżeli na jakimś portalu społecznościowym wpisujemy swoją edukację, warto się zastanowić, czy musimy podawać tam datę, bo prawdopodobnie ten profil jest otwarty. Na przykład na LinkedInie. I czy to ma takie wielkie znaczenie, kiedy kończyliśmy którą szkołę. To znaczy, to nie ma żadnego znaczenia - chyba, że bardzo chcemy odnaleźć kolegów i koleżanki z klasy. Ale jeżeli nie, no to to jest duża informacja, bo można w tym momencie próbować wyszukiwać informacje o nas, które już nam się wydaje, że dawno nie istnieją. Na przykład Nasza Klasa już nie istnieje, ale informacje z jej czatów wciąż są wyszukiwalne przez Google. No podobnie jest z ustalaniem wtedy daty urodzenia. To znaczy, jeśli wiem, kiedy Pani miała maturę, to jestem w stanie z dużym przybliżeniem określić datę urodzenia danego człowieka. Naprawdę, Internet jest przepastny. Możliwości wyszukiwania są ogromne i coś, co kiedyś wrzuciliśmy do sieci… Też warto zwrócić uwagę, że kiedyś były inne standardy wyszukiwania, to znaczy ja mogłam wrzucić na Chomika parę lat temu dużo różnych informacji, i nikt nie był w stanie ich wyszukać. Dzisiaj zadaję pytanie do Google i przeszukuję Chomika, także to jest zupełnie co innego. Więc każda informacja, którą sobie dorzucamy, powinna być przemyślana. Nie zawsze trzeba to robić.

[00:25:40 Patrycja Długoń] Jeżeli porobiliśmy te błędy w przeszłości, a teraz nasza świadomość jest większa, to co? Zostawić? Usunąć, jak i tak tam zostanie?

[00:25:51 Karolina Małagocka] To jest trochę tak, że oczywiście jak coś już w Internecie się pojawia, to się mówi, że ono na zawsze zostanie, ale może nie ułatwiajmy jednak pracy tym, którzy chcieliby się o nas dużo dowiedzieć. Tak, no mamy problemy kolejne… nie chciałam już otwierać kolejnych drzwi do coraz… Bo cyberbezpieczeństwo trochę jest jak ta czarna dziura z powieści o Alicji, czyli zaglądamy i ona jest coraz czarniejsza i coraz głębsza. No, ale na przykład problem ze stalkerami, czyli z osobami, które coraz częściej prześladują innych. Jeżeli nie muszą te informacje tam być, to uczyńmy je trochę ciężej dostępnymi. To znaczy, jeżeli coś można wykasować, to mimo wszystko dobrze jest to wykasować. Jeżeli już chcemy korzystać z portali randkowych, to zdjęcie nie takie samo, jak na profilu na LinkedInie. Naprawdę łatwo jest wyszukać kogoś po zdjęciu, można próbować oszukiwać te algorytmy. Ja nie mówię, że ma być zdjęcie, które kapeluszem zasłania całą twarz, to byłoby najlepsze, ale jeżeli już nawet chcemy pokazać swoje zdjęcie, to nie takie samo jak mamy, nie wiem… na profilu na LinkedInie, czy na przykład na naszej stronie internetowej w firmie, czy gdziekolwiek indziej. Jeżeli naprawdę nie jest to kluczowe, kiedy zdawaliśmy maturę, albo kiedy kończyliśmy jakieś studia, to te daty należy całkowicie usunąć. Ja bym też je usunęła, powiem zupełnie szczerze, ponieważ niezwykle często teraz algorytmy decydują o zatrudnieniu, a te algorytmy mają swoje bajpasy, więc po co… po cóż nam te informacje, kiedy ktoś kończył studia. Ważne, że je skończył i myślę, że chyba nie ma takiego znaczenia, kiedy to się wydarzyło, a pozwala naprawdę nawet na wydedukowanie wielu innych informacji.

[00:27:37 Patrycja Długoń] Wspominała Pani o tych zagrożeniach w przyszłości, grupowaniu się niebezpiecznych osób, które później przechodzić mogą do działania. Jakie jeszcze zagrożenia Pani widzi *a propos* przyszłości, jeżeli chodzi o dezinformacje?

[00:27:58 Karolina Małagocka] Jeżeli chodzi o samą dezinformację to myślę, że faktycznie będziemy coraz bardziej podatni. To znaczy będziemy coraz bardziej żyli w dwóch światach, a właściwie to będzie za chwilę jeden świat, to znaczy… już dzisiaj ciężko mi jest powiedzieć, jaka jest różnica między „off” i „on”, i czy my na pewno jesteśmy kiedykolwiek „off-line”, bo właściwie cały czas jesteśmy „on-line”, więc te nasze przyzwyczajenie do tego, co się w tym świecie „on-line” dzieje… Kiedyś się wydawało, że jak się coś czytało w Internecie to, to było mniej wiarygodne niż to, co powiedziano w telewizji, radiu i co można było przeczytać w prasie. Dziś coraz częściej mówimy sobie, że Internet jest lepiej poinformowany. Warto zwrócić uwagę, że w Internecie każdy może napisać wszystko, nie ponosi za to żadnej odpowiedzialności, często też nawet się pod tym nie podpisuje. Więc, wydaje mi się, że będziemy na to narażeni, jeśli chodzi o to ile informacji o nas będzie zbieranych, i że my możemy stać się jakby źródłem tworzenia „deep fake’ów”. No to tutaj wszelkiego rodzaju nasze przyzwyczajenie do bycia publicznym, to znaczy do poszerzania sobie kręgu znajomych o ludzi nieznajomych, to myślę, że będzie też duże zagrożenie. Będziemy coraz bardziej dostępni - nasz głos, nasz wizerunek. Właściwie dzisiaj ciężko mi jest sobie przypomnieć osobę, do której zdjęcia nie można dotrzeć w taki lub inny sposób, albo danych nie można namierzyć w Internecie. Więc to będzie tak, że stanie się to nam bliższe, to znaczy, że możemy my się stać ofiarą nawet takiego rewanżu. Dzisiaj rozmawiamy o tym „revange pornie”, który się pojawia - to jest ogromnym stygmatem dla ofiary. No, ale możemy sobie wyobrazić takie „deep fake’owe” informacje robione już na mikro skalę, czyli dzisiaj rozmawiamy o tym, że może to być jakaś wielka machina finansowana prawdopodobnie przez rząd takiego lub innego państwa. Za chwilę będzie to na tyle tanie i dostępne, że mogę sobie wyobrazić, że koleżanka koleżance, kolega koledze - będzie mógł zorganizować taką kampanię oszczerstw, i to będzie po prostu wykonalne. Wydaje mi się, że bardzo dużo jest do zrobienia w zakresie edukacji dzieci. Dzisiaj mówimy, że mamy problem z hejtem w Internecie, czyli że ktoś coś źle napisał o koledze, koleżance, ale to się jakoś odnosi do rzeczywistości. Ja jestem sobie w stanie wyobrazić, że naszą przyszłością niestety mogą być „hejterskie fake newsy”, czyli że to nie dość, że będzie duża kampania nienawiści, to jeszcze zupełnie nieprawdziwa. Więc zdecydowanie wydaje mi się, że takie krytyczne myślenie o tym, co do mnie dociera, i co ja oglądam na własne oczy, i słyszę na własne uszy - musimy młodym ludziom wpajać. Jeżeli chodzi o zagrożenia w ogóle takie ogólne - wydaje mi się, że Internet rzeczy to jest taki kolejny problem, który możemy mieć.

[00:30:52 Patrycja Długoń] Co to jest Internet rzeczy?

[00:30:54 Karolina Małagocka] No to będą te nasze wszystkie inteligentne przedmioty podłączone do sieci, którym będziemy się otaczali, już się otaczamy tak? Czyli kamerki, czyli odkurzacze, czyli… nie wiem, inteligentne domy. No warto zwrócić uwagę, że te przedmioty będą podłączone do sieci, one będą miały oprogramowanie - to oznacza, że to będzie komputer z funkcją czyszczącą, czy też komputer z funkcją piorącą. Nie dość, że będzie nas można zaatakować to będzie nas można podsłuchiwać – właśnie. No i na nieszczęście nasze będzie nas można obserwować. I o ile nie wierzę, że ktoś będzie przejmował mikrofalówkę żeby zabić kogoś, bo jakby… są łatwiejsze sposoby pozbawienia kogoś życia, i na koniec -pozbawianie życia jest jednak we wszystkich chyba krajach nielegalne, a przynajmniej zagrożone karą i to dość surową. O tyle obawiam się, że może być to świetny sposób do właśnie różnego rodzaju takich pomniejszych akcji, czy to agresywnych, czy to właśnie mających na celu zbieranie informacji o nas. Warto zwrócić uwagę, że niestety ta technologia trochę idzie w kierunku dawania oczu i uszu coraz większej ilości przedmiotów.

[00:32:08 Patrycja Długoń] Pani Karolino, pięknie dziękuję za tę fascynującą rozmowę, czego mogę Pani na koniec życzyć?

[00:32:41 Karolina Małagocka] Ja bym chciała, żeby technologia, za którą płacimy, respektowała nasze prawo, które mamy, czyli i do wyboru, i do prywatności, i do tego, że nie chcemy być powszechnie inwigilowani przez każdego, kto ma odpowiednie zasoby. Więc myślę, że to bym bardzo chciała. I bardzo bym chciała, żeby tych negatywnych zjawisk - przy całym pięknie technologii - było coraz mniej, żeby to nasze marzenie, które mieliśmy, jak żeśmy tą technologię tworzyli, czyli że nie powtórzą się te błędy z XX wieku, czyli że będzie więcej wiedzy i więcej zrozumienia dla świata, i to nas uczyni lepszymi społeczeństwami - żeby to się faktycznie sprawdziło, bo na razie ten scenariusz nie jest aż taki optymistyczny.

[00:32:59 Patrycja Długoń] To tego właśnie Pani życzę, i jeszcze raz dziękuję.

[00:33:02 Karolina Małagocka] Dziękuję bardzo.

[00:33:06 Patrycja Długoń] Moją rozmówczynią w policyjnym cyklu rozmów z ekspertami Wspólnie Bezpieczniej - była doktor Karolina Małagocka z Akademii Leona Koźmińskiego w Warszawie. Więcej informacji o dezinformacji znajdziecie Państwo w linkach, które umieściliśmy w opisie do pierwszej części tej rozmowy, oraz w kwietniowym numerze Gazety Policyjnej, który dostępny będzie już niedługo pod adresem gazeta.policja.pl. Zapraszam do subskrybowania naszych podcastów i bardzo dziękuję za uwagę, Patrycja Długoń.

[00:33:41] Koniec.

Opracowanie WPP BKS KGP, Warszawa 2022

SK / pd