WYWIAD Z MIKE'IEM MALSCHEM, SZEFEM BIURA FBI W POLSCE

Mike Malsch, Szef Biura FBI w Polsce opowiada o zagrożeniach i wyzwaniach związanych z rozwojem nowych technologii. Opisuje także działania amerykańskich instytucji w obszarze cyberbezpieczeństwa, priorytetach FBI i współpracy międzynarodowej.

Kasia Sokół: Mike, to wyjątkowa okazja móc porozmawiać z Agentem FBI, opowiedz proszę, o swojej karierze w FBI.
Kasia Sokół

Mike Malsch: Zacząłem pracę w FBI w 2004r. Nie marzyłem o pracy w FBI . Z wykształcenia jestem informatykiem i po studiach, przez 11 lat, pracowałem jako programista komputerowy.

Wstrząsające wydarzenia, które miały miejsce 11 września 2001r. spowodowały, że ponownie przeanalizowałem wybór zawodu. Nigdy wcześniej nie służyłem w wojsku ani w żadnej instytucji publicznej, więc zacząłem szukać sposobów, aby wykorzystać swoje umiejętności w służbie mojego kraju. Po roku poszukiwań i rozważań różnych opcji, złożyłem podanie do FBI. Od tego momentu do otrzymania zaproszenia do Akademii Szkoleniowej FBI w Quantico w stanie Virginia, minęły prawie 2 lata. Ukończyłem Akademię jako Agent Specjalny FBI i rozpocząłem nową ścieżkę kariery.

Obecnie mamy do czynienia z deficytem specjalistów z dziedziny informatyki. Jako ekspert ds. cyberbezpieczeństwa, czy masz jakieś sugestie, co można zrobić i jak zachęcić młodych ludzi do wyboru kariery w tej dziedzinie? Jakie byłoby Twoje przesłanie do nich?

Masz rację – istnieje ogromne zapotrzebowanie na tego typu wiedzę specjalistyczną, ponieważ wyzwania związane z cyberbezpieczeństwem rosną z każdym dniem. Podnosisz również słuszną kwestię dotyczącą zachęcania do wyboru cyberbezpieczeństwa jako ścieżki kariery. Tak wiele naszych codziennych interakcji odbywa się z wykorzystaniem aplikacji i systemów komputerowych. Na naszych urządzeniach przechowujemy plany zajęć, kontakty, wiadomości, dokumenty, muzykę i rozrywkę oraz wiele innych danych. Ochrona tych informacji ma zasadnicze znaczenie dla bezpieczeństwa.

Z tego powodu uważam, że zachęcanie dzieci do komputerów powinno rozpocząć się wcześnie i obejmować nie tylko edukację w zakresie korzystania z nich, ale także ochrony informacji. Jeśli dzieci będą szanować wartość swoich danych, zrozumieją, jak ważna jest ich ochrona.

Dodatkowo, jako funkcjonariusz organów ścigania, mam pewną satysfakcję z prowadzenia dochodzeń i stawiania przed sądem osób, które postanowiły przywłaszczyć sobie informacje, które do nich nie należą.

Poza wykształceniem istnieją inne czynniki zachęcające do podjęcia pracy w dziedzinie cyberbezpieczeństwa – dobre wynagrodzenie, pewność zatrudnienia, ciągłe wyzwania związane z rozwiązywaniem nowych problemów oraz satysfakcja ze świadomości, że przyczyniasz się do zapewnienia bezpieczeństwa innym.

Jesteś w Polsce od ponad dwóch lat, zajmując się różnego rodzaju przestępstwami, które mają związek z USA lub po prostu wspierając polskich partnerów.

Tak, zapewniamy wsparcie polskim służbom w zwalczaniu cyberprzestępczości, ale jednocześnie wykorzystujemy informacje uzyskane od naszych polskich partnerów do zwalczania cyberprzestępczości w USA. Wspieramy się także w innych obszarach. Jak wiadomo, w cyberprzestępczości nie ma granic. W dzisiejszych czasach, partnerstwo jest niezbędnym elementem walki z przestępczością. Cieszę się, że mamy tak świetną współpracę z naszymi polskimi partnerami, tutaj w Polsce.

**Jednym z głównych zadań NASK jest cyberbezpieczeństwo więc, jeśli nie masz nic przeciwko temu, chciałabym się skupić na tym obszarze Twojej pracy.
Jakie są aktualnie główne priorytety FBI? Kilka lat temu zwalczanie cyberprzestępczości było w pierwszej piątce.**

Bezpieczeństwo Amerykanów przed terroryzmem – zarówno międzynarodowym jak i krajowym, jest na pierwszym miejscu priorytetów FBI. Natomiast zgodnie z obowiązującą strategią, cyberprzestępczość jest jednym z naszych najwyższych priorytetów.

Wykorzystujemy ogólnokrajowe zasoby – naszą obecność i naszych ludzi – do aktywizacji i większego angażowania partnerów. Nie tylko dobrze znanych, dużych przedsiębiorstw, ale także tych mniejszych, które stanowią podstawę naszej infrastruktury krytycznej.

Chcemy szybko dzielić się informacjami z partnerami, ale chcemy też, aby oni dzielili się z nami właściwymi informacjami. Chcemy, aby nasi partnerzy stanowili dla nas i dla bezpieczeństwa kraju czynnik zwielokrotniający siłę, ponieważ wszyscy bierzemy na siebie wspólną odpowiedzialność za obronę przed cyberprzestępcami. Dużo informacji jest dla nas niedostępnych, bo należą do podmiotów z sektora prywatnego, więc musimy być godnym zaufania partnerem, żeby ta współpraca miała sens.

Jakie zmiany zauważyłeś w ostatnich latach, jeśli chodzi o cyberprzestępczość?

Oprogramowanie ransomware jest coraz bardziej ukierunkowane, precyzyjne i coraz bardziej dochodowe z punktu widzenia sprawców. Liczba incydentów zgłoszonych do IC3 w 2020 roku wzrosła o 20%, natomiast straty pieniężne wynikające z tych incydentów wzrosły o 225%. Statystyki te nie obejmują kosztów związanych z zakłóceniem działalności biznesowej i usuwaniem skutków, które mogą przewyższać wysokością kwotę żądanego okupu.

Jeśli jest coś, w czym FBI jest szczególnie wyspecjalizowane, to jest to zwalczanie przestępczości zorganizowanej i wszelkich organizacji przestępczych. W kwestii ransomware i ich skutecznej neutralizacji współpracujemy z bezprecedensową w historii liczbą organizacji sektora rządowego i prywatnego.

Zakłócanie działania przestępców poprzez ich identyfikację, także tych znajdujących się za granicą, ich infrastruktury i przepływu pieniędzy ma kluczowe znaczenie w walce z oprogramowaniem ransomware. Najtrwalszy efekt osiągniemy, gdy zakłócimy działanie wszystkich tych elementów razem, oraz gdy połączymy możliwości i zasoby nasze oraz naszych partnerów.

Cyberprzestrzeń i reagowanie na incydenty to sport zespołowy. Skuteczne reagowanie na zagrożenia wymagają podejścia typu „wszystkie ręce na pokład", a w skład takiego zespołu wchodzą partnerzy zagraniczni, sektor prywatny, a nawet indywidualne osoby.

FBI zdecydowanie odradza ofiarom płacenie przestępcom okupu. Spełnienie żądań nie gwarantuje, że cyberprzestępca odszyfruje Twoje pliki lub dotrzyma obietnicy, że nie zrobi nic ze skradzionymi danymi.

Zapłacone w ramach okupu pieniądze działają jak dolanie benzyny do ognia. Nie uda nam się opanować problemu, dopóki nie będzie mniej tego rodzaju „paliwa" dla przestępców.

Warto również zauważyć, że w przypadku kradzieży danych, często widzimy, że przestępcy powtórnie atakują te same firmy.

Rozumiem jednak, że płacenie lub niepłacenie to trudna decyzja. Spędziłem wiele czasu w sektorze prywatnym, pomagając firmom w podejmowaniu trudnych decyzji – czasem nawet ma się wrażenie, że nie ma innego wyjścia, jak tylko zapłacić.

Jakie są obecnie główne wyzwania związane z cyberbezpieczeństwem i cyberzagrożeniami? Jakie są Twoje przewidywania na przyszłość?

Szczególne miejsce pod względem wagi i istotności w hierarchii FBI w tej sferze stanowią zagrożenia ze strony podmiotów i grup finansowanych wspieranych przez państwa. Jest tak przede wszystkim z uwagi na stosowanie przez nich zaawansowanych i potencjalnie destrukcyjnych metod, a także wytrwałość w przygotowaniach i działaniach. Ransomware stanowi jeden z przykładów oprogramowania, mającego bez wątpienia najbardziej widoczny i bezpośredni, negatywny wpływ na amerykańską infrastrukturę krytyczną, w tym szpitale, sektor energetyczny i służby ratownicze.

Nasza strategia opiera się w duże mierze na budowaniu silnych powiązań z sektorem prywatnym i na przekazywaniu informacji o zagrożeniach naszym partnerom, zanim staną się bezpośrednim celem ataku cyberprzestępców.

Przez lata nasi przeciwnicy uprawiali cyberszpiegostwo w celu gromadzenia danych, a także brali na cel naszą infrastrukturę krytyczną. Obecnie media społecznościowe stały się bardzo sprawnym narzędziem w ich rękach. Poprzez media mogą mieć wpływ na to, jak się zachowujemy i jakie podejmujemy decyzje. W miarę, jak łączymy i integrujemy miliardy nowych urządzeń cyfrowych z naszym życiem i procesami biznesowymi, przestępcy mogą uzyskać większy wgląd w nasze chronione informacje i dostęp do nich.

Ostatnie głośne przypadki incydentów o dużej skali, takich jak SolarWinds, Hafnium, Pulse Secure i Colonial Pipeline, pokazują, jak wiele czasu, pieniędzy i wysiłku poświęcają przeciwnicy, aby nam zaszkodzić – zarówno podmioty i grupy finansowane lub wspierane przez państwa, jak i cyberprzestępcy.

Liczba i skala poważnych incydentów rośnie z każdym dniem i stanowi wyzwanie dla naszej wspólnej zdolności reagowania.

Co ważne, nie postrzegamy przestępców i podmiotów państwowych w kategoriach „albo-albo".

To, co wyróżnia FBI, to fakt, że mamy uprawnienia do prowadzenia śledztw i gromadzenia danych operacyjnych dotyczących zarówno przestępstw, jak i zagrożeń ze strony podmiotów państwowych.

To, co widzimy w tej pracy, to wymieszane zagrożenia, gdzie często nie ma jasnej linii, gdzie kończy się działalność cyberprzestępcza, a zaczyna działalność podmiotów sponsorowanych przez inne państwa. W zależności od potrzeb one się przenikają i wzajemnie wykorzystują. Przestępcy sprzedają swoje usługi, a podmioty finansowane przez państwa używają narzędzi i technik typowych dla cyberprzestępców, aby ukryć swoją działalność. Żadna agencja nie jest w stanie samodzielnie rozwiązać tak dużego i trudnego problemu, jakim są cyberzagrożenia.

Znajdujemy się w samym środku ekosystemu broniącego kraju, dysponując zasobami sięgającymi od głębokich powiązań z sektorem prywatnym, po narzędzia charakterystyczne dla służb wywiadowczych. Wykorzystujemy ten szeroki zakres aktywności do zbierania informacji na temat przestępców i sposobów ich powstrzymywania, opracowywania danych operacyjnych, których my i nasi partnerzy potrzebujemy do wspólnego, zaplanowanego działania – uderzając w podmioty za pomocą wszelkich środków, od zatrzymań, przez likwidację infrastruktury sektora rządowego i prywatnego, po sankcje, naciski dyplomatyczne i inne środki w celu osiągnięcia maksymalnego i skoordynowanego efektu. Żadne z narzędzi naszego systemu prawnego nie działa bez określonego celu i wystarczających dowodów uzasadniających podjęcie działań.

Przeciwdziałamy cyberzagrożeniom na dwa różne sposoby: pierwszy to zapobieganie i zakłócanie, a drugi to przekazywanie informacji naszym partnerom, którzy są w stanie podjąć najbardziej efektywne i skuteczne działania w celu neutralizacji zagrożenia.

Największa różnica między cyberśledztwami, a innymi działaniami jest rola sektora prywatnego, dlatego dostarczamy przedsiębiorstwom i środowiskom akademickim różnych rodzajów ważnych informacji – od strategicznych ostrzeżeń o zamiarach przeciwnika, przez taktyczne, konkretne informacje o wskaźnikach, których obrońcy sieci potrzebują, aby się chronić, po indywidualne ostrzeżenia o tym, że aktorzy obierają ich za cel lub aktywnie ich atakują.

W dużej mierze polegamy również na tym, co sektor prywatny może nam powiedzieć o tym, co widzi w kontrolowanych przez siebie sieciach, w których znajduje się niemal cała infrastruktura krytyczna, informacje personalne i własność intelektualna, chroniona przez FBI.

W jaki sposób FBI przyczynia się do promowania współpracy międzynarodowej i budowania partnerstw w dziedzinie cyberbezpieczeństwa i zwalczania cyberprzestępczości?

Większość naszych przeciwników i ich infrastruktury znajdują się za granicą, więc współpraca międzynarodowa jest niezwykle istotna. FBI ściśle współpracuje zarówno z innymi amerykańskimi agencjami, jak i partnerami zagranicznymi, aby skutecznie wykorzystywać zasoby do zwalczania cyberterrorystów, ograniczając ich możliwości, a także zapobiegając cyberatakom na podmioty amerykańskie.

Dzięki współpracy krajowej i międzynarodowej FBI z powodzeniem przerwało działalność wielu operacji przestępczych w sieciach komputerowych.

Wykorzystujemy zdobytą wiedzę i możliwości i dzielimy się nimi z naszymi partnerami, tak abyśmy mogli wspólnie wykorzystać wszystkie dostępne narzędzia.

Jeśli chodzi o zasięg międzynarodowy to ponieważ cyberprzestrzeń nie ma granic, FBI musi mieć zasięg globalny. Oficerowie Łącznikowi FBI ds. cyberprzestępczości (ALAT) stacjonujący w ambasadach na całym świecie pomogli zbudować koalicje „podobnie myślących krajów", które wspierają USA w walce z naszymi przeciwnikami. W ramach tego programu nasi Agenci ds. cyberprzestępczości pracują w strategicznych placówkach budując zaufanie z naszymi zagranicznymi partnerami na całym świecie. Dzielimy się informacjami, koordynujemy działania i dochodzimy sprawiedliwości dla ofiar cyberprzestępstw.

FBI może również korzystać z pomocy międzynarodowych partnerów w celu zlokalizowania skradzionych danych lub zidentyfikowania sprawcy incydentu.

Przykładem tego typu współpracy może być skoordynowana międzynarodowa operacja, mająca na celu przerwanie działania botnetu Emotet, który był wykorzystywany przez przestępców do uzyskania dostępu do ponad miliona komputerów na całym świecie i sprzedawania tego dostępu innym, w tym grupom zajmującym się oprogramowaniem ransomware. Podejmując skoordynowane działania na skalę globalną, znacznie utrudniliśmy przestępcom ponowne utworzenie sieci.

Jeśli chodzi o zwalczanie ransomware to budujemy w tym zakresie nową i pogłębioną współpracę międzynarodową w celu rozbicia ekosystemu tego oprogramowania z udziałem krajów partnerskich poprzez rozbijanie struktur finansowania działalności przestępców oraz poprzez prowadzenie bezpośrednich działań dyplomatycznych w celu rozwiązania problemu tzw. „bezpiecznych przystani", jurysdykcji w których sprawcy czują się jak gdyby byli poza zasięgiem organów ścigania, w szczególności przestępcy rozwijający lub wykorzystujący oprogramowanie ransomware.

Czy FBI jest jedyną agencją wywiadowczą zajmującą się cyberprzestępczością w USA? Czy może macie jakiś zakres lub podział kompetencji?

FBI jest główną agencją federalną zajmującą się reagowaniem na zagrożenia. Nasze dochodzenia koncentrują się na gromadzeniu dowodów w celu ustalenia, kim są hakerzy, gdzie i jak działają, kto ich wspiera oraz jakie działania będą miały największy wpływ na przeciwdziałanie ich poczynaniom. Kiedy więc doradzamy lub współpracujemy z sektorem prywatnym, wykorzystujemy naszą wiedzę o zagrożeniach, aby sprawdzić, w jaki sposób firma może stać się celem ataku, jak jej systemy są wzajemnie połączone oraz jaki jest najlepszy sposób ochrony przed zagrożeniami, z którymi prawdopodobnie się zetknie. Przykładem mogą być informacje o wektorze ataku, czyli o tym, gdzie zdaniem organizacji znajdował się podatny punkt, który umożliwił cyberprzestępcom naruszenie bezpieczeństwa systemu.

Mamy szczęście mieć w USA dwie krajowe agencje, CISA (Cybersecurity&Infrastructure Security Agency) i FBI (Federal Bureau of Investigation), o bardzo różnych uprawnieniach i możliwościach, których role wzajemnie się uzupełniają, a które współpracując ze sobą, wzmacniają naszą obronę cyberprzestrzeni w sposób, jaki nie mógłby mieć miejsca, gdyby ze sobą konkurowały lub były odizolowane.

Mocną stroną CISA jest zajmowanie się podatnościami w cyberprzestrzeni, oceną ryzyka oraz wzmacnianiem odporności i obrony stron internetowych w domenie .gov oraz infrastruktury krytycznej.

FBI przekazuje informacje, które gromadzi dzięki unikalnemu połączeniu kompetencji w zakresie zwalczania przestępczości i bezpieczeństwa krajowego, których może pozazdrościć wielu partnerów za granicą, a także dzięki fizycznej obecności na terenie USA, która umożliwia bliską współpracę z podmiotami, zanim dojdzie do niepożądanego zdarzenia, oraz z ofiarami, gdy niestety do niego dojdzie.

Raz ujawnione informacje dają CISA możliwość zidentyfikowania innych sieci podatnych na tę samą technikę – mogą przekazać FBI, CYBER COMMAND lub NSA fragment infrastruktury podmiotu, który można zakłócić lub wykorzystać. Dzięki temu National Security Council (Rada Bezpieczeństwa Narodowego) wie, w jaki sposób wykorzystać wszystkie posiadane instrumenty władzy przeciwko osobom odpowiedzialnym za dany atak.

Bez względu na to, skąd informacje trafiają do podmiotów rządowych, ważne jest, aby CISA i FBI miały równe możliwości dostępu do nich i działania na ich podstawie w ramach swoich zadań.

Bez względu na sposób w jaki się zorganizujemy i działamy, FBI pozostaje odpowiedzialne za prowadzenie śledztw w sprawach dotyczących cyberprzestępczości, postawienia winnych przed obliczem wymiaru sprawiedliwości.

Jaka jest rola Centrum Zwalczania Przestępczości Internetowej FBI (Internet Crime Complaint Center – IC3)? W jaki sposób jego praca i obowiązki mogą wpłynąć na europejski ekosystem cyberbezpieczeństwa, np. w Polsce i ogólnie w UE?

Współcześnie FBI jest agencją bezpieczeństwa krajowego wykorzystującą dane wywiadowcze i koncentrującą się na zagrożeniach dla bezpieczeństwa naszego kraju, ale jednocześnie jest częścia organów ścigania, agencją zwalczającą przestępczość. Skupiamy się na ochronie obywateli amerykańskich przed terroryzmem, szpiegostwem, cyberatakami, poważnymi zagrożeniami kryminalnymi, a także na zapewnieniu partnerom usług, wsparcia i szkoleń. IC3 służy realizacji tych potrzeb jako narzędzie gromadzące informacje na temat cyberprzestępczości, dzięki czemu możemy działać prewencyjnie i przewidzieć potencjalne zagrożenia.

IC3 zostało utworzone w maju 2000 roku w celu przyjmowania zgłoszeń dotyczących przestępstw internetowych. Od momentu powstania otrzymało ponad 6,5 miliona zgłoszeń. Misją organizacji jest zapewnienie społeczeństwu wiarygodnego i prostego mechanizmu zgłaszania do FBI informacji dotyczących podejrzeń działalności przestępczej w cyberprzestrzeni oraz rozwijania współpracy z organami ścigania i partnerami branżowymi.

Zebrane informacje są analizowane i rozpowszechniane w celach operacyjnych i wywiadowczych dla organów ścigania oraz w celu zwiększenia świadomości społecznej. Do tego celu, IC3 opracowuje coroczny raport, który ma na celu edukację społeczeństwa w zakresie trendów mających wpływ na jego funkcjonowanie.

Jakość danych wynika bezpośrednio z informacji wprowadzanych za pomocą publicznego interfejsu – www.ic3.gov, oraz z danych skategoryzowanych na podstawie informacji podanych w poszczególnych skargach. Pracownicy IC3 analizują zebrane dane, w celu określenia trendów w cyberprzestępczości i ich wpływu na społeczeństwo w nadchodzącym roku.

Jaką rolę w USA odgrywa National Cyber Investigative Joint Task Force (NCIJTF)? Jaka jest rola FBI w tej strukturze?

W celu stawienia czoła coraz większym wyzwaniom związanym z cyberprzestępczością, w 2008 r. powołano do życia National Cyber Investigative Joint Task Force (NCIJTF). NCIJTF składa się z ponad 30 amerykańskich podmiotów z uprawnieniami organów ścigania, zaangażowanych w działalność wywiadowczą oraz Departamentu Obrony, których przedstawiciele są rozmieszczeni w różnych miejscach i wspólnie pracują nad realizacją misji organizacji z perspektywy całego rządu.

Jako jedyne w swoim rodzaju centrum cyber, zrzeszające wiele agencji lub instytucji, NCIJTF jest odpowiedzialne za koordynację, integrację i wymianę informacji w celu wspierania śledztw oraz obsługi incydentów dotyczących cyberzagrożeń, a także dostarczania i wspierania sporządzania analiz wywiadowczych.

NCIJTF harmonizuje również wspólne działania, skupiające się na identyfikowaniu i ściganiu terrorystów, szpiegów i przestępców, którzy próbują wykorzystać lub zaatakować systemy informatyczne naszego kraju.

W USA istnieje wiele wspólnych inicjatyw lub organów, których celem jest dzielenie się i wymiana informacji. Wygląda na to, że wyciągnęliście wnioski po 11 września, ale okazało się, że jest to też skuteczne narzędzie pracy. Wspomnieliśmy już o IC3 i NCIJTF.
Czy możesz nam opowiedzieć o Krajowym Sojuszu na rzecz Cyberbezpieczeństwa i Szkoleń (National Cyber-Forensic and Training Alliance, NCFTA)?

National Cyber-Forensic and Training Alliance (NCFTA) został założony w 2002 r. jako partnerski sojusz typu non-profit pomiędzy sektorem prywatnym, publicznym i środowiskiem akademickim wyłącznie w celu zapewnienia neutralnego, zaufanego środowiska, które umożliwia dwukierunkową współpracę w zakresie identyfikacji, łagodzenia skutków i zakłócania cyberprzestępczości. NCFTA koncentruje się na wynikach. Dzięki stworzeniu środowiska, w którym partnerzy ufają sobie nawzajem i swobodnie dzielą się informacjami, NCFTA była w stanie zapobiec potencjalnym stratom w wysokości prawie 2 miliardów dolarów, a także pomóc w identyfikacji krytycznych zagrożeń dla sektora prywatnego. NCFTA wspiera również globalne wysiłki organów ścigania, pomagając w identyfikacji bieżących zagrożeń, które mają największy wpływ na sektor prywatny. Trzy główne obszary zainteresowania NCFTA to: ochrona marki i konsumentów, zagrożenia finansowe oraz złośliwe oprogramowanie i cyberzagrożenia.

NCFTA jest globalnym modelem partnerstwa publiczno-prywatnego, współpracy, wzajemnego wsparcia i zaufania bez względu na granice czy sektory. Poprzez ciągłe posze-

rzanie relacji partnerskich z organami ścigania, przedstawicielami sektora prywatnego, partnerami z ośrodków akademickich z kraju jak i z zagranicy, NCFTA wciąż zwiększa swoje możliwości operacyjne i ulepsza infrastrukturę i możliwości techniczne.

Czy Twoim zdaniem skuteczniejsza jest scentralizowana czy zdecentralizowana walka z cyberprzestępczością (działania stanowe vs. federalne, a w Polsce: regionalne/wojewódzkie vs. krajowe)?

Trudno jest odpowiedzieć na to pytanie ze względu na różnice w strukturze i systemach prawnych pomiędzy Polską a USA. Mogę jedynie powiedzieć, że wiedza specjalistyczna będzie się rozwijać w sposób zdecentralizowany, ponieważ śledczy zajmujący się cyberprzestępczością napotykają różne scenariusze w prowadzonych przez siebie sprawach. Zagrożenia także będą się ujawniać w sposób zdecentralizowany, ponieważ cyberprzestępcy działają bez względu na strukturę organów ścigania. Niezależnie od formalnej struktury, elastyczność i zdolność do adaptacji pozostają kluczowymi kompetencjami w zwalczaniu cyberprzestępczości.

Jakbyś zdefiniował największe zagrożenia związane z wykorzystywaniem nowych technologii przez przestępców? Która z technologii Twoim zdaniem najbardziej przyczyniła się do ułatwienia popełniania przestępstw?

Stosowanie nowych technologii przez cyberprzestępców może ograniczyć zdolność organów ścigania do wykrywania, identyfikowania i łagodzenia skutków użycia nowych technik i taktyk. Przestępcy mogą przez pewien czas cieszyć się z ich perspektywy niczym nieograniczonymi sukcesami, podczas gdy metody działania organów ścigania, m.in. w zakresie gromadzenia informacji oraz ograniczania negatywnych skutków przestępczości, będą ewoluować. Zgłaszające się ofiary mogą nie być w stanie opisać sposobu, w jaki padły ofiarą.

Kiedy poruszamy temat cyberprzestępczości i cyberbezpieczeństwa, nierozerwalnie łączy się to także z rozprzestrzenianiem fake newsów i dezinformacji. Czy FBI zajmuje się tą problematyką? Jeśli tak, to w jaki sposób?

Jesteśmy zaniepokojeni wzrostem popularności operacji z wykorzystaniem złośliwego oprogramowania lub tzw. operacji wpływu.

Szybkie tempo rozwoju technologii z zakresu sztucznej inteligencji i uczenia maszynowego, wykorzystywanych do generowania treści – obrazów, materiałów audio, wideo lub tekstu – prawdopodobnie wyprzedzi rozwój możliwości ich wykrywania i atrybucji.

Tak wygenerowane treści mogą być wykorzystywane jako nowy wektor cyberataku, określanego jako Business Identity Compromise i który stanowi wersję rozwojową techniki Business Email Compromise, wykorzystującą zaawansowane techniki i nowe narzędzia. BIC obejmuje wykorzystanie narzędzi do generowania treści i manipulacji w celu wykreowania „sztucznych", nieistniejących w rzeczywistości pracowników lub stworzenia zaawansowanej lecz fałszywej tożsamości istniejącego pracownika. Wygenerowane, spreparowane treści mogą być również wykorzystywane do atakowania osób lub grup szczególnie podatnych na ataki, takich jak dzieci.

Ten wektor ataku może mieć znaczący wpływ na finanse oraz reputację firm i organizacji, które padły jego ofiarą. Współpracujemy z naszymi partnerami z różnych agencji oraz z sektorem prywatnym, aby działać prewencyjnie wobec tego problemu.

Kilka czynników wpłynęło na zmniejszenie zasobów, czasu i wysiłków wymaganych do stworzenia lub wykorzystania przekonujących wygenerowanych treści. Oznacza to, że metody niegdyś dostępne tylko dla osób dysponujących sprzętem o odpowiedniej mocy obliczeniowej i wiedzą fachową, mogą być obecnie stosowane przez szersze grono podmiotów za pośrednictwem przyjaznych dla użytkownika w obsłudze aplikacji. Jedną

z konsekwencji tego trendu jest to, że tworzenie treści wygenerowanych przez algorytmy stało się w zasadzie usługą, a same treści – towarem i wykracza to poza niegdyś ograniczone zastosowania.

Wizualne zniekształcenia i wypaczenia lub niespójności w obrazach i wideo mogą wskazywać na to, że obrazy zostały wygenerowane, zwłaszcza w przypadku profili w mediach społecznościowych.

W identyfikacji i ocenie podejrzanych treści mogą pomóc niezależne organizacje badawcze i kryminalistyczne, a także niektóre renomowane firmy zajmujące się cyberbezpieczeństwem.

Osoby fizyczne i organizacje mogą zmniejszyć ryzyko rozpowszechniania spreparowanych i nieprawdziwych treści, stosując odpowiednie zasady cyberhigieny i inne środki bezpieczeństwa. Wskazane jest zachowanie czujności i zdrowego rozsądku podczas korzystania z informacji online, zwłaszcza gdy tematy są szczególnie kontrowersyjne lub podburzające.

Należy także poszukiwać wielu niezależnych źródeł podawanej informacji w celu jej weryfikacji, przeszkolić pracowników lub użytkowników, aby rozpoznawali i zgłaszali próby wykorzystania socjotechniki i spearphishingu, zarówno wobec ich kont osobistych jak i firmowych. Dobrze byłoby też opracować i przećwiczyć plany ciągłości komunikacji na wypadek, gdyby konta w mediach społecznościowych zostały przejęte i wykorzystane do rozpowszechniania wygenerowanych lub fałszywych treści.

Powszechnie już wiadomo, że nie należy otwierać załączników ani klikać łączy w wiadomościach elektronicznych otrzymanych od nierozpoznanych nadawców, nie należy podawać danych osobowych, w tym nazw użytkownika, haseł, dat urodzenia, numerów PESEL, danych finansowych ani innych informacji w odpowiedzi na zapytania z nieznanego źródła.

Należy zachować ostrożność przy przekazywaniu poufnych informacji osobistych lub firmowych drogą elektroniczną lub telefoniczną. Jeśli to możliwe, należy potwierdzić prośbę o poufne informacje za pośrednictwem innych kanałów.

Należy zawsze sprawdzać adresy internetowe prawdziwych witryn i wpisywać je ręcznie do przeglądarki.

FBI prowadzi szeroką kampanię informacyjną, zachęcając osoby i organizacje, które podejrzewają, że mogły paść ofiarą cyberprzestępstwa, lub posiadają informacje o podejrzanej lub przestępczej działalności cybernetycznej, do skontaktowania się z lokalnym biurem terenowym FBI lub złożenia szczegółowej skargi w Centrum Zwalczania Przestępczości Internetowej IC3.

Muszę zapytać o wojnę na Ukrainie. Wiem, że nie możemy mówić o szczegółach, ale czy masz więcej pracy od czasu wybuchu wojny?

Niestety nie mogę udzielić odpowiedzi na to pytanie. Mogę jedynie podzielić się treścią oficjalnych komunikatów FBI dotyczących wojny na Ukrainie:

- „FBI jest zaangażowane w badanie i zwalczanie wszelkich incydentów z wykorzystaniem złośliwego oprogramowania, mających wpływ na infrastrukturę krytyczną Ukrainy. Współpracujemy z naszymi partnerami w kraju i za granicą, aby zidentyfikować i powstrzymać te ukierunkowane cyberzagrożenia. Nasi Oficerowie Łącznikowi FBI w Europie i na całym świecie odgrywają kluczową rolę we wspieraniu i wymianie informacji z naszymi ukraińskimi i międzynarodowymi partnerami."

- Oficjalny komunikat dotyczący zagrożeń wewnętrznych: „FBI, wraz z naszymi partnerami federalnymi, pozostaje zaangażowane w badanie i zwalczanie wszelkiego rodzaju cyberprzestępstw wymierzonych w Stany Zjednoczone. FBI konsekwentnie rozpowszechnia publiczne ostrzeżenia

o zagrożeniach, ostrzegające o działaniach prowadzonych przez podmioty lub grupy powiązane z Rosją. Nadal aktywnie dzielimy się informacjami z naszymi partnerami z sektora prywatnego, aby identyfikować cele i zapobiegać incydentom. Zachęcamy społeczeństwo do zgłaszania wszelkich podejrzanych działań na adres www.ic3.gov."

Jakie są główne wyzwania związane z Twoją pracą w Polsce?

Uważam, że główne wyzwania związane z pracą w Polsce są podobne do tych, które można znaleźć w każdej pracy związanej z egzekwowaniem prawa w większości innych krajów, w tym w Stanach Zjednoczonych.

Pracując nad śledztwami z naszymi partnerami, często grzęźniemy w obciążeniach administracyjnych i ograniczeniach prawnych, które nie nadążają za rozwojem technologicznym w cyberprzestrzeni. Nie mówię tu o kwestiach gwarantowanych przez nasze Konstytucje – wolności słowa, wyznania, zgromadzeń, prasy, ochronie przed nieuzasadnionymi przeszukaniami i zatrzymaniami, sprawiedliwych procesach sądowych itp. Mam na myśli obciążenia związane z wymogami papierkowej roboty, przepisów, które odnoszą się do starszej technologii, ale pomijają aspekty nowszej i które nie zapewniają odpowiedniej kary dla przestępców. Aby odnieść sukces w dziedzinie cyberbezpieczeństwa, konieczne jest zsynchronizowanie technik dochodzeniowych z procesami prokuratorskimi oraz dostosowanie do nich wyroków sądowych.

Mike, bardzo dziękuję za rozmowę.