Ministerstwo
Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.159.2024
Warszawa, 27 stycznia 2025 r.

Szanowny Pan
Szymon Hołownia
Marszałek Sejmu RP

Dot. pisma z 19 grudnia br. Posłów na Sejm RP Panów Dariusza Mateckiego, Andrzeja Śliwki, Dariusza Stefaniuka, Michała Wosia oraz Przemysława Drabka w sprawie działań Ministerstwa Cyfryzacji na rzecz zwalczania podszywania się pod osoby publiczne w mediach społecznościowych (interpelacja nr 7030)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Posłów pytania.

Ad 1) Czy Ministerstwo Cyfryzacji prowadzi obecnie rozmowy z właścicielami globalnych platform społecznościowych, takich jak Meta, Google czy X, w celu wprowadzenia bardziej skutecznych mechanizmów walki z fałszywymi kontami?

CSIRT NASK[1] - Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego poziomu krajowego, przygotował pakiet wytycznych, które zostały przekazane firmie Meta, pozwalający znacząco podnieść bezpieczeństwo Polaków korzystających z serwisów społecznościowych tej firmy (Facebook, Instagram). Znalazły się tam oczekiwania: zatrudnienia polskich moderatorów, blokowania użytkowników, których reklamy były oznaczone jako oszustwo, korzystania z listy ostrzeżeń[2], o której szerzej w odpowiedzi na pyt. 2 i innych źródeł danych pochodzących od lokalnych partnerów, wyspecjalizowanych w wyszukiwaniu zagrożeń na danym rynku. Działania te pozwolą usprawnić filtrowanie złośliwych linków zewnętrznych pojawiających się na ich platformach, a także uporządkowanie biblioteki reklam. Oczekujemy od firmy Meta przedstawienia planu wdrożenia skutecznego rozwiązania wykrywającego szkodliwe treści w języku polskim.

Ad 2) Czy planowane jest stworzenie krajowych regulacji, które wymusiłyby na globalnych podmiotach podejmowanie bardziej stanowczych działań w celu ochrony tożsamości użytkowników z Polski?

Ochrona tożsamości użytkowników w Polsce jest regulowana przez rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietna 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[3], zwane dalej „RODO", które obowiązuje w całej Unii Europejskiej. RODO nakłada na wszystkie podmioty przetwarzające dane osobowe obywateli UE, w tym także właścicieli globalnych platform społecznościowych, obowiązek zapewnienia odpowiedniego poziomu ochrony tych danych. Przepisy te nakładają na administratorów danych osobowych oraz podmiotów przetwarzających zapewnienie integralności i poufności danych osobowych. Szczególnie istotne są tutaj przepisy art. 32

[1] Obowiązki CSIRT NASK, o których mowa w ustawie z dn. 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2024 r. poz. 1077) zostały powierzone zespołowi CERT Polska funkcjonującego w strukturze Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego (NASK-PIB) nadzorowanego przez Ministra Cyfryzacji.
[2] https://cert.pl/lista-ostrzezen/
[3] Dz. Urz. UE L 119 z 4.5.2016, str. 1 ze zm.

telefon +48 22 245 54 42
adres email sekretariat.BM@cyfra.gov.pl
www.gov.pl/web/cyfryzacja

ul. Królewska 27
00-060 Warszawa

RODO i art. 28 RODO, zgodnie z którymi administrator danych osobowych oraz podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne mające zapewnić stopień bezpieczeństwa danych osobowych odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych.

W Polsce wprowadzono również dodatkowe przepisy, zawarte w ustawie o zwalczaniu nadużyć w komunikacji elektronicznej[4], mające na celu przeciwdziałanie kradzieży tożsamości. Na poziomie ustawowym została umocowana lista ostrzeżeń, o której mowa w odp. na pyt. 1 dotyczących domen internetowych, które służą do wyłudzeń danych i środków finansowych użytkowników internetu. Lista ostrzeżeń przed niebezpiecznymi domenami prowadzona jest przez Zespół CERT Polska. W każdym przypadku stwierdzenia zagrożenia, które może prowadzić do wyłudzenia danych, np. strona podszywająca się pod portal społecznościowy, domena jest dodawana na listę ostrzeżeń. W 2024 r. Zespół CERT Polska wykrył i dodał na ww. listę 3700 stron podszywających się pod portal Facebook (Meta), których celem było wyłudzenie danych logowania.

Jednym z kluczowych działań mających na celu ochronę tożsamości użytkowników platform społecznościowych jest monitorowanie i analiza zagrożeń, które mogą wpływać na bezpieczeństwo użytkowników danej platformy. NASK-PIB[5] w ramach swoich zadań ustawowych i statutowych, monitoruje na bieżąco ataki mające na celu wyłudzenie danych oraz prowadzi liczne kampanie uświadamiające w tym temacie na portalach społecznościowych, które szerzej opisano w odp. na pyt. 4.

Ad 3) Czy Ministerstwo zamierza opracować krajowy system zgłaszania i monitorowania przypadków podszywania się w mediach społecznościowych, który byłby zintegrowany z działaniami organów ścigania?

Założenie konta na dane osobowe innej osoby narusza atrybut autentyczności danych (właściwość, która polega na tym, że podmiot jest tym, za kogo się podaje). Takie zdarzenie kwalifikuje się jako incydent w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa[6]. Zgodnie z art. 30 tejże ustawy, osoby fizyczne mogą zgłosić taki incydent do CSIRT NASK, który jest z kolei obowiązany współpracować z organami ścigania i wymiaru sprawiedliwości oraz służbami specjalnymi przy realizacji ustawowych zadań, a więc m.in. przy zwalczaniu cyberprzestępczości.

Ad 4) Jakie kroki podejmuje Ministerstwo, aby edukować obywateli na temat rozpoznawania i zgłaszania fałszywych kont?

Ministerstwo Cyfryzacji, we współpracy ze wspomnianym wyżej NASK-PIB, realizuje wiele działań edukacyjnych z zakresu cyberbezpieczeństwa, które są kierowane do różnych grup użytkowników internetu. Działania te uwzględniają również aspekty bezpiecznego korzystania z mediów społecznościowych. W ramach tych działań NASK-PIB prowadzi kampanie informacyjne w zakresie bezpiecznego korzystania z Internetu. NASK-PIB opracowuje i publikuje materiały edukacyjne dot. różnego rodzaju oszustw internetowych, w tym oszustw na fałszywe inwestycje (Uważaj na fałszywe inwestycje w sieci), które często wykorzystują wizerunek osób publicznych.

NASK-PIB uruchomił również możliwość zgłaszania treści i profili, które noszą znamiona działań dezinformacyjnych. Inicjatywa ta nosi nazwę #WŁĄCZWERYFIKACJĘ.[7] Tego typu treści można zgłaszać na adres: informacje@nask.pl. Zgłoszone treści są weryfikowane przez doświadczonych ekspertów, którzy ocenią potencjalne przejawy działań

[4] ustawa z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (Dz. U. z 2023 r. poz. 1703)
[5] Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy nadzorowany przez Ministra Cyfryzacji
[6] ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2024 r. poz. 1077)
[7] https://www.nask.pl/pl/aktualnosci/4411,WlaczWeryfikacje-NASK-przeciw-dezinformacji-w-sieci.html

dezinformacyjnych. Na podstawie zweryfikowanych zgłoszeń NASK-PIB informuje o przypadkach dezinformacji, równocześnie przedstawiając rzetelne informacje o zagadnieniach, których dotyczyła nieprawdziwa wiadomość. Działania te prowadzone są zarówno w serwisie Facebook (Meta), jak i na Platformie X (Twitterze). W przypadku gdy określone treści wypełniają znamiona czynu zabronionego, wówczas informowane są również organy ścigania, które podejmą działania w celu wykrycia sprawcy.

Ponadto, na portalu gov.pl rozwijana jest baza wiedzy cyberbezpieczeństwa[8], gdzie publikowane są praktyczne poradniki (m.in. poradnik „Bezpieczni w mediach społecznościowych"), artykuły, rekomendacje oraz inne materiały edukacyjne, które pozwalają społeczności internetowej zdobyć wiedzę na temat bezpiecznego korzystania z technologii cyfrowych i jak chronić się przed cyberzagrożeniami.

Realizowane są również projekty wpierające nauczanie o bezpieczeństwie online: „CYBER lekcje"[9] oraz „Bezpieczni w Sieci"[10] skierowane do uczniów szkół podstawowych i ponadpodstawowych. Celem tych projektów jest edukacja o cyberbezpieczeństwie dopasowana do aktualnych trendów funkcjonowania dzieci i młodzieży w internecie oraz cyberzagrożeń, z którymi stykają się najmłodsi użytkownicy sieci m.in. w mediach społecznościowych.

Jednocześnie, Ministerstwo Cyfryzacji prowadzi intensywne działania informacyjne dotyczące zgłaszania incydentów cyberbezpieczeństwa i prób oszustw. Wszystkie próby oszustw internetowych należy zgłaszać do Zespołu CERT Polska. Zgłoszenia można dokonać poprzez formularz na stronie https://incydent.cert.pl lub wysyłając e-mail na adres cert@cert.pl. Fałszywe wiadomości SMS można zgłosić używając funkcji "przekaż" albo "udostępnij" na numer 8080.

Z wyrazami szacunku
Paweł Olszewski
Sekretarz Stanu
/dokument podpisany elektronicznie/

Do wiadomości:
Kancelaria Prezesa Rady Ministrów - Departament Spraw Parlamentarnych

[8] https://www.gov.pl/web/baza-wiedzy/aktualnosci
[9] https://www.gov.pl/web/baza-wiedzy/materialy-do-cyberlekcji
[10] https://bezpieczniwsieci.edu.pl/