fundacja instytut
CYBERBEZPIECZEŃSTWA

Doxing i swatting

- na czym polegają te sposoby cyberprzemocy i czy można się przed nimi chronić?

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości

Wzrost powszechnego dostępu do Internetu i rozwój technologii przyniosły ze sobą liczne korzyści, ale wraz z tym postępem pojawiły się także zagrożenia związane z cyberprzemocą. Zjawisko to obejmuje m.in. doxing i swatting, czyli dwie niebezpieczne formy przemocy, mogące wyrządzić poważne szkody zarówno wirtualnie, jak i w rzeczywistości. Zrozumienie tych zagrożeń oraz skuteczne metody ochrony przed nimi stają się istotne, aby zapewnić bezpieczeństwo w erze cyfrowej.

Doxing

Doxing jest formą cyberprzemocy polegającą na gromadzeniu i wykorzystywaniu zebranych w Internecie danych na temat innych osób. Samo określenie pochodzi od słów z j. angielskiego, takich jak *docs* (dokumenty) oraz *releasing* (przetwarzać, upubliczniać)[1]. Doxerzy wyszukują w sieci informacje na temat konkretnej osoby, sprawdzają jej aktywność i zbierają różne dane, a potem upubliczniają informacje na temat tej osoby, np. jej dane osobowe, miejsce zamieszkania czy numer telefonu. Zjawisko to związane jest z wyszukiwaniem informacji w Internecie, które zostały już upublicznione przez daną osobę. Nie polega zatem na ataku hakerskim na urządzenia czy skrzynkę mailową w celu wykradzenia danych, a na pozyskiwaniu danych, które ktoś już udostępnił. Doxerzy zatem śledzą aktywność danej osoby w sieci. Internauci pozostawiają wiele śladów np. poprzez udostępnianie zdjęć lub relacji w mediach społecznościowych, polubienie lub udostępnienie konkretnych postów czy zostawianie komentarzy. Często udostępniają też na swój temat bardzo dużo danych, np. na Facebooku lub w serwisie LinkedIn, publikując swoją datę i miejsce urodzenia, miejsce zamieszkania, adres mailowy oraz inne informacje. Dane pozyskane w ramach doxingu mogą zostać wykorzystane przeciwko tej osobie. Zdarzają się łagodne formy żartu, mające na celu zawstydzenie innej osoby, ale doxing może wiązać się także z poważnym przestępstwem, mającym na celu ośmieszenie, zdyskredytowanie lub zniesławianie ofiary oraz wywołanie u niej poczucia zagrożenia, a nawet wykluczenie jej z przestrzeni publicznej. Ofiarą doxingu może paść każdy, a najbardziej narażone na niego są osoby znane, np. politycy, dziennikarze, aktywiści, youtuberzy, celebryci oraz influencerzy. Doxerzy wyszukują wiele różnych danych, a te informacje, które są wyszukiwane najczęściej, przedstawia poniższa grafika.

Doxerom zależy na wyrządzeniu krzywdy danej osobie przez udostępnienie jej da-

1 Doxing – nowe zjawisko i (cyber)zagrożenie, https://www.gov.pl/web/baza-wiedzy/doxing--nowe-zjawisko-i-cyberzagrozenie (dostęp 30.08.2023).

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości

nych. Poza przedstawionymi na grafice informacjami będą zatem interesować ich wszelkie informacje, których dana osoba nie chciałaby udostępniać. Może to być jakieś wydarzenie z przeszłości, zdjęcie lub nagranie, którego ktoś nie chce upublicznić.

Popularnym przykładem doxingu były działania prowadzone przez rosyjskich cyberprzestępców w stosunku do fińskiej dziennikarki Jessikki Aro, która zidentyfikowała i donosiła o prokremlowskich trollach na długo przed tym, jak stali się oni powszechnie poruszanym tematem. Rosyjscy propagandyści ujawnili jej historię medyczną, adres domowy oraz teledysk wyśmiewający ją jako „dziewczynę Bonda"[2]. Twierdzili również bezpodstawnie, że była prostytutką oraz dilerką narkotyków. W tym przypadku zatem doxing został połączony z dezinformacją, aby w jak największym stopniu zaszkodzić dziennikarce.

Ofiarą doxingu może paść każdy, komu ktoś chce zaszkodzić i mimo że trudno jest całkowicie ochronić się przed doxerami, warto zachować bezpieczeństwo i ostrożność w sieci, aby potencjalny cyberprzestępca mógł pozyskać jak najmniej danych. Poniżej przedstawiono kilka wskazówek, w jaki sposób chronić się przed doxingiem[3]:

2 N. Jankowicz i. in, Malign Creativity: How Gender, Sex, and Lies are Weaponized Against Women Online, Wilson Center, 2021, https://www.wilsoncenter.org/publication/malign-creativity-how-gender-sex-and-lies-are-weaponized-against-women-online (dostęp 30.08.2023).

3 A. Kuszner, Czym jest doxing? jak możesz się przed nim uchronić?, NASK, https://

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości

- nie ujawniaj w Internecie wrażliwych danych osobowych,
- uważaj na zdjęcia i nagrania video, które publikujesz w Internecie,
- usuń stare konta w mediach społecznościowych, z których już nie korzystasz,
- ustaw odpowiednie ustawienia dotyczące prywatności w mediach społecznościowych,
- nie publikuj dużej ilości informacji dotyczących życia prywatnego,
- sprawdź, jakie informacje ktoś w chwili obecnej mógłby znaleźć na Twój temat w Internecie i usuń te, których nie chcesz upubliczniać.

Swatting

Inną formą cyberprzemocy jest swatting, czyli generowanie nagłej reakcji organów ścigania przeciwko ofierze. Termin ten pochodzi od nazwy SWAT (Special Weapons and Tactis), czyli specjalnej jednostki policji w USA. Zjawisko to polega na tym, że przestępca dzwoni na policję i przekazuje nieprawdziwe informacje o tym, że konkretna osoba stwarza poważne zagrożenie, np. posiada broń i kogoś postrzeliła, przechowuje narkotyki albo popełniła inne przestępstwo. Jego celem jest doprowadzenie do interwencji policji w związku z tą osobą . Swatting staję się coraz popularniejszy w USA i może mieć poważne konsekwencje.

Przykładem takiego zjawiska jest wydarzenie z 2017 r. w Wichita. Wówczas dwóch graczy *Call of Duty: WWII* pokłóciło się. Jeden z nich uznał, że naśle na drugiego SWAT i skontaktował się z osobą, którą poprosił o zadzwonienie na policję i przekazanie fałszywych informacji. Taki telefon został wykonany, a dzwoniący na policję Tyler Barriss podał się za jednego z graczy i powiedział, że zabił swojego ojca i kieruje broń przeciwko pozostałym członkom rodziny. Dodał, że oblał cały dom benzyną i podpali go, jeżeli przyjedzie policja[4]. Podał także adres zamieszkania, w którym miał się znajdować, będąc przekonanym, że podaje adres zamieszkania jednego z graczy. W rzeczywi-

cyberprofilaktyka.pl/blog/0/czym-jest-doxing-jak-mozesz-sie-przed-nim-uchronic_i25.html (dostęp 30.08.2023).

4 M. Smith, Fatal 'Swatting' Episode in Kansas Raises Quandary: Who Is to Blame?, New York Times, 2017, https://www.nytimes.com/2017/12/31/us/wichita-swatting-barriss.html (dostęp 30.08.2023).

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości

stości należał on do przypadkowej osoby. Kiedy policja przyjechała pod dom, wyszedł z niego zaskoczony mężczyzna, który wykonywał nerwowe ruchy. Jeden z policjantów oddał strzał, w obawie, że sięga po broń. Strzały te okazały się śmiertelne, a ofiarą padła niewinna osoba. W 2019 r. sąd skazał Barrissa na 20 lat więzienia.

Innym przykładem swattingu było wykorzystanie tego rodzaju ataku przeciwko streamerce Clarze Sorrenti[5]. Ktoś podszywając się pod nią, wysłał maila do ratusza w Londynie, w którym informował o posiadaniu karabinu i chęci ataku na ratusz. Sprawę przekazano policji, a ta, myśląc, że streamerka planuje atak z bronią na ratusz, wysłała do jej domu specjalny oddział, który ją zatrzymał oraz skonfiskował jej telefony i komputery. Sorrenti ostatecznie wypuszczono. Istnieją podejrzenia, że akcja z fałszywem mailem była częścią kampanii, którą przeprowadzały nękające ją na Twitchu trolle. Swatting to zjawisko, przed którym ciężko się chronić. Kluczowe w przeciwdziałaniu przestępstwom tego typu są skuteczne działania policji.

Swatting nie jest jeszcze popularny w Polsce, ale biorąc pod uwagę rosnącą popularność influencerów oraz youtuberów, zjawisko to może także dotrzeć do Polski. Dotychczas w Polsce zdarzały się jednak podobne sytuacje, jednak stwarzające mniejsze zagrożenie, polegające na zamówieniu pizzy, mebli, a nawet prostytutek pod adres innej osoby.

Podsumowanie

Doxing i swatting to dwie różne formy cyberprzemocy, które stanowią poważne zagrożenie. Ofiarą doxingu może paść każdy, kto udostępnia w sieci dużo informacji o sobie. Doxer, który znajdzie odpowiednie dane może je wykorzystać w celu zaszkodzenia konkretnej osobie. Bardzo ważne w ochronie przed tym zagrożeniem jest ostrożne korzystanie z Internetu i nieudostępnianie wrażliwych informacji. Swatting natomiast obecnie występuje głównie w USA, a jego ofiarami padają najczęściej celebryci i influencerzy. Zjawisko to może jednak pojawić się w przyszłości także w Polsce.

5 A. Khan, Red flags aplenty in London police's swatting of Twitch streamer Clara Sorrenti: expert, Global News, 2022, https://globalnews.ca/news/9069338/london-police-swatting-twitch-streamer-clara-sorrenti-keffals/ (dostęp 30.08.2023).

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości

Bibliografia:

1. *Doxing – nowe zjawisko i (cyber)zagrożenie*, https://www.gov.pl/web/baza-wiedzy/doxing--nowe-zjawisko-i-cyberzagrozenie (dostęp 30.08.2023).
2. Jankowicz N. i. in, *Malign Creativity: How Gender, Sex, and Lies are Weaponized Against Women Online*, Wilson Center, 2021, https://www.wilsoncenter.org/publication/malign-creativity-how-gender-sex-and-lies-are-weaponized-against-women-online (dostęp 30.08.2023).
3. Khan A., *Red flags aplenty in London police's swatting of Twitch streamer Clara Sorrenti: expert*, Global News, 2022, https://globalnews.ca/news/9069338/london-police-swatting-twitch-streamer-clara-sorrenti-keffals/ (dostęp 30.08.2023).
4. Kuszner A., *Czym jest doxing? jak możesz się przed nim uchronić?*, NASK, https://cyberprofilaktyka.pl/blog/0/czym-jest-doxing-jak-mozesz-sie-przed-nim-uchronic_i25.html (dostęp 30.08.2023).
5. Smith M., *Fatal 'Swatting' Episode in Kansas Raises Quandary: Who Is to Blame?*, New York Times, 2017, https://www.nytimes.com/2017/12/31/us/wichita-swatting-barriss.html (dostęp 30.08.2023).

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości

www.instytutcyber.pl

fundacja instytut
CYBERBEZPIECZEŃSTWA

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości