KONSPEKT

TEMAT SPOTKANIA: Bezpieczeństwo danych i anonimowość w sieci

CEL: Świadomość, że korzystanie z sieci przez szeregowego użytkownika tylko pozornie zapewnia anonimowość. Budowanie umiejętności podnoszenia stopnia bezpieczeństwa przechowywanych przez nas danych

ZAKRES TREŚCI:

1. Wstęp
2. Cyfrowy ślad
3. Prywatność i wolność słowa, a prawo do anonimowej wypowiedzi
4. Czy moje dane są bezpieczne?
5. Przykłady praktyczne - ćwiczenia

WYNIKI:

1. Rozumienie, że domyślne ruch sieciowy nie jest anonimowy
2. Podniesienie świadomości obywatelskiej odnośnie prawa do anonimowej wypowiedzi
3. Umiejętność zabezpieczenia posiadanych danych
4. Kształtowanie dobrych praktyk podczas korzystania z sieci

1. Wstęp

Jedną z cech internetu jest jego anonimowość, co nie oznacza anonimowości absolutnej. Dowodem na brak całkowitej anonimowości jest ściganie przestępstw, które są popełniane za pośrednictwem sieci.

Czy zawsze jednak anonimowość w sieci służy do popełniania przestępstw, a osoby domagające się jej powinny być piętnowane za domaganie się jej?

Coraz częściej wśród komentarzy mówi się o prawie użytkowników do anonimowej wypowiedzi online, która ma stanowić odzwierciedlenie wolności słowa w internetowej rzeczywistości.

W pewnym stopniu z prawem do bycia anonimowym w sieci powiązane jest również bezpieczeństwo naszych danych (rozumianych nie tylko jako treści znajdujące się na urządzeniu, za pomocą którego komunikujemy się z internetem, ale również hasła i materiały udostępniane przez nas na portalach społecznościowych i chmurach), ponieważ zabezpieczenie posiadanych przez nas danych uniemożliwia dostęp do nich niepożądanym osobom. Czy zwyczajny użytkownik zdaje sobie w ogóle sprawę z potrzeby ochrony tych danych?

Rozpytanie uczniów/uczestników

Na samym początku warto zapytać uczestników/uczniów o to, czy przywiązują wagę do swojej anonimowości w sieci? Czy zależy im na utrzymaniu takiej anonimowości? Czy spotkali się z sytuacją, kiedy dana osoba działając z pozoru anonimowo została zdemaskowana? Jak do tego

doszło? Czy zabezpieczają posiadane przez siebie dane? Czy poza standardowymi zabezpieczeniami stosują jeszcze inne środki? Podane przez uczniów odpowiedzi można zapisać na tablicy.

2. Cyfrowy ślad

Duża część użytkowników internetu w ogóle nie zdaje sobie sprawy, że każde korzystanie z sieci buduje nasz cyfrowy ślad, dzięki któremu możliwe jest odtworzenie naszych ruchów sieciowych.

Zatem każda wizyta na portalu społecznościowym, wysyłanie wiadomości przez komunikator lub pocztę elektroniczną, wyrażanie zgód w ramach polityk prywatności, publikacja komentarzy na forach, portalach i serwisach pozostaje w zasobach sieci i może zostać odtworzona.

W zdecydowanej większości przypadków to śledzenie służy poznaniu przez algorytmy wyszukiwarek naszego profilu, dostosowywać rodzaj pokazywanych reklam, aby jak najlepiej odpowiadały naszym preferencjom (były dla nas interesujące).

Już na pierwszy rzut oka widać, że np. wyszukiwanie produktów w popularnym portalu ogłoszeniowym lub sklepie internetowym powoduje się wyświetlanie po późniejszym czasie w oknach reklamowych na innych stronach internetowych tych lub podobnych propozycji zakupowych do tych, które w niedalekiej przeszłości wynajdowaliśmy.

Część niezorientowanych użytkowników jest błędnie przekonana o tym, że usunięciu śladu cyfrowego służy m.in. wprowadzony do przeglądarek tryb incognito nazywany trybem prywatnym, podczas gdy poza usunięciem popularnych ciastek i historii przeglądania nasza aktywność (odwiedzane strony) widoczna jest na zewnątrz (np. widzi ją dostawca usług).

W pewnym zakresie mamy wpływ na stopień śledzenia naszego ruchu i jeżeli zależy nam na prywatności, może ograniczyć ilość przekazywanych informacji lub korzystać z urządzeń, które redukują ilość przekazywanej treści.

Warto pamiętać, że dzięki cyfrowemu śladowi możliwe jest ściąganie przestępstw popełnionych za pośrednictwem internetu.

Z pozoru może się wydawać, że ujęcie sprawcy takiego przestępstwa jest niemożliwe, natomiast główną przeszkodzą na drodze do ujęcia sprawcy jest brak szczegółowych informacji na temat jego działań. Z Kolei analiza ruchu sieciowego przez administratorów serwisów pozwala na ustalenie danych osób, które mogłyby dopuścić się przestępstwa.

W prowadzonych postępowaniach karnych może być badane prawdopodobieństwo (na podstawie formy budowania loginu, hasła, podawanych danych teleadresowych, numeru telefonu, czy danych zabezpieczających konto), czy grupa stworzonych kont sprzedawców może należeć do tej samej osoby. W powiązaniu z tym, że konta służą do podobnych działań (np. sprzedaż internetowa biletów) i zgłoszeniami nabywców o nieprawidłowościach w transakcji możemy w łatwy sposób powiązać jedną osobę lub grupę współpracujących ze sobą osób z danym przestępstwem.

3. Prywatność i wolność słowa, a prawo do anonimowej wypowiedzi

Jak już było wspomniane na samym początku, z prawem do anonimowej wypowiedzi będąc online utożsamiana jest wolność słowa w internecie.

Ponadto anonimowość związana jest z potrzebą zapewnienia naszego prawa do prywatności, które jest dobrem osobistym chronionym polskimi przepisami.

Oczywiście można postawić tezę, która pojawia wśród przeciwników takiego rozumowania, że będąc w sieci powinniśmy akceptować i dostosowywać się do pewnych reguł, które są nam narzucane przez regulaminy serwisów lub przepisy. W wypadku serwisów komercyjnych, portali tworzonych przez osoby fizyczne lub firmy, które uzależniają dostęp do publikowanych przez nich treści od rejestracji jest to zrozumiałe.

Z inną sytuacją mamy natomiast do czynienia, kiedy mówimy o portalach publicznych (np. serwisy miast), które miałyby ograniczać nam prawo do wypowiadania się o określonych faktach z uwagi na brak podania przez nas szczegółowych danych osobowych. Tytułem analogii można podać, że w ramach realnej dyskusji otwartej prowadzonej przy okazji wykładu, odczytu, spotkania z artystą nasza możliwość zabrania głosu nie jest uzależniona od przedstawienia swoich danych identyfikujących, a jedynie dopuszczenia nas do głosu.

Odnośnie życia prywatnego rolą anonimowości jest uzewnętrznienie naszych poglądów (w sposób, który nie będzie uznany za bezprawny) bez narażenia się na ingerencję organów na skutek tego, że w sposób nieprzychylny, kontestujący zabieramy głos względem sprawy nas interesującej.

W wypadku anonimowości realizującej postulat wolności słowa intuicyjnie kierujemy swoją uwagę w stronę mediów i dostrzegamy potrzeby ich niezależności. Prawo do anonimowej publikacji (brak podania nazwiska autora kontrowersyjnego materiału powstałego na skutek prowadzonego śledztwa dziennikarskiego) ma przede wszystkim ułatwiać mediom rolę tzw. *watchdoga* (psa stróżującego) jako niezbędnego elementu istniejącego we współczesnych demokracjach.

Spory o istnienie potrzeby anonimowości jako cechy środowiska wirtualnego pojawiały się w przeszłości na tyle często, że również w orzeczeniach polskiego wymiaru sprawiedliwości natrafimy na rozważania na ten temat.

Dzisiaj dość zdecydowanie obecne jest stanowisko (o czym wypowiedział się w przeszłości również Sąd Najwyższy), że powszechnie przyjętą zasadą i istotą usługi dyskusyjnego portalu internetowego jest anonimowość usługobiorców korzystających z ogólnie dostępnych internetowych portali dyskusyjnych, których zadaniem jest zapewnienie przede wszystkim swobody wypowiedzi, co jest przecież zasadniczym celem takich portali.

Nie można oczywiście zapominać, że prawo do bycia anonimowym nie może służyć nam publikacji treści szkodliwych i bezprawnych, które ograniczają prawa i wolności innych i narażają nas na odpowiedzialność.

4. Czy moje dane są bezpieczne?

Teraz właśnie jest najlepszy moment na weryfikację, czy przechowywane przez nas dane (czy to na dysku fizycznym, czy w chmurze) są bezpieczne. Przede wszystkim sprawdź:

- Czy posiadane oprogramowanie antywirusowe i zapora sieciowa są aktualne
- Czy korzystam z menadżera haseł
- Czy używam weryfikacji dwuetapowej, kiedy jest oferowana
- Czy korzystam z wtyczek umożliwiających wymuszanie połączenia szyfrowanego
- Jaki jest stan wyeksploatowania dysku fizycznego (stopień zużycia), aby w porę przenieść dane na nowy nośnik
- Czy w chmurze przechowywane są dane wrażliwe, których nie chcemy ujawnić
- Czy w komunikatorach, mailach lub smsach ujawniane są dane wrażliwe
- Czy posiadam kopie zapasowe najważniejszych danych

Nie zapominajmy również o tym, że formą budowania poczucia bezpieczeństwa na temat naszych danych znajdujących się w sieci jest pełna informacja o naszych prawach jako użytkowników względem danych i możliwościach ich przetwarzania. Zgody nie muszą być udzielone wieczyście. Kiedy przestajemy interesować się jakąś stroną, warto zastanowić się nad wycofaniem uprzednio udzielonej zgody.

5. Przykłady praktyczne - ćwiczenia

PRZYKŁAD I

Blog obywatelski założony w celu publikacji wpisów o lokalnych problemach w małej społeczności. Pod kolejnymi artykułami pojawiają się anonimowe wpisy skierowane wprost do przedstawicieli władz – wytykające błędy, niegospodarność, popełnianie przestępstw. Prowadzącemu blog zarzucono niewłaściwe skonstruowanie formuły komentarzy bez potrzeby rejestracji użytkownika, z powodu której wysoce utrudnione jest ustalenie autorów nieprzychylnych wpisów. Czy obowiązek taki faktycznie istnieje?

Tego rodzaju sprawa faktycznie była rozpoznawana przez polski wymiar sprawiedliwości. Polskie sądy uznały, że administrator bloga był obowiązany do skonstruowania mechanizmu publikacji wpisów w taki sposób, aby była możliwa weryfikacja użytkowników.

W sprawie prowadzonej już przez międzynarodowy sąd – Europejski Trybunał Praw Człowiek w Strasburgu ze względu na złożenie skargi jednak ustalono, że pierwszeństwo powinna znaleźć zasada prawa do anonimowej wypowiedzi online, a ograniczenia w tym względzie (obowiązek rejestracji) naruszałyby wolność słowa w internecie.

Nie zmienia to jednak faktu, że administrator po powzięciu wiedzy o pojawieniu się na blogu komentarza, który jest bezprawny (narusza przepisy) powinien niezwłocznie go usunąć.

Warto tutaj zwrócić uwagę na kontekst samej sprawy i to, że niepochlebne wpisy pojawiały się w ramach małej społeczności lokalnej. W takim środowisku możliwość anonimowego wyrażenia zdania jest jedyną szansą na zabranie głosu w ramach prowadzonej dyskusji na tematy publiczne.

PRZYKŁAD II

Na portalu internetowym jednego z popularnych tygodników pojawił się artykuł dotyczący naruszający dobra osobistej osoby trzeciej. Autor materiału nie podpisał się imieniem i nazwiskiem, ponieważ chciał pozostać anonimowy. Osoba, której dotyczy artykuł wystąpiła do gazety z wnioskiem o udostępnienie danych osobowych autora artykułu, ponieważ chciałaby wystąpić na drogę cywilną ze sprawą o ochronę dóbr osobistych. Czy prawo do anonimowości autora góruje nad prawem do ochrony względem osoby, której dotyczy artykuł?

O zasadach publikacji materiałów prasowych mówi ustawa prawo prasowe. W jednym z artykułów jest mowa o tym, że autorowi materiału prasowego (a do takiego można zaliczyć artykuł opublikowany na portalu internetowym tygodnika) przysługuje prawo do zachowania w tajemnicy swoje nazwiska (art. 15 ustawy). Motywacja autora nie ma tutaj znaczenia.

Nie oznacza to jednak, że osoba dotknięta treścią niepochlebnego artykułu nie ma żadnych możliwości dochodzenia ochrony naruszonych dóbr osobistych, ponieważ odpowiedzialność cywilną za naruszenie prawa spowodowane opublikowaniem materiału prasowego obok autora ponoszą również redaktor lub inna osoba, która spowodowała opublikowanie materiału. Odpowiedzialność tych osób jest solidarna (art. 38 ustawy).

Prawo do domagania się ochrony dóbr osobistych nie musi się zatem odbywać kosztem wyłączenia anonimowości autora materiału prasowego.

PRZYKŁAD III

Podczas codziennego korzystania z komputera zauważyliśmy, że ktoś niepowołany uzyskał dostęp do naszej skrzynki poczty elektronicznej, która posłużyła mu do rozsyłania spamu do kolejnych odbiorców. Po zawiadomieniu policji i sprawdzeniu numeru IP, z którego nastąpiło logowanie do poczty okazało się, że sprawca działał z ogólnodostępnej sieci bezprzewodowej jednego z lokali gastronomicznych? Czy właściciel lokalu odpowiada w tej sytuacji?

To prawda, że obecnie istnieją narzędzia geolokalizacyjne, ale ich zastosowanie w praktyce w wielu wypadkach okazuje się znacznie utrudnione lub też nie przynosi efektów w postaci ustalenia osoby, przeciwko której należy prowadzić postępowanie.

Samodzielnie nie mamy praktycznie żadnych możliwości ustalenia sprawcy włamania na nasze konto mailowe.

W toku postępowania, które prowadzi policja pojawia się szansa na takie ustalenia, ale proces uzyskiwania informacji, które są niezbędne dla ustalenia danych podmiotu dokonującego

włamania jest obarczony licznymi ograniczeniami, które ostatecznie mogą doprowadzić do fiaska poszukiwań.

Właściciel lokalu, który w ramach swojej działalności udostępnia sieć bezprzewodową klientom jest traktowany jako dostawca usługi i nie powinien ponosić odpowiedzialności za działania osób z niej korzystających.

Nie zmienia to jednak faktu, że dostawca usługi (właściciel łącza) powinien współpracować z organami prowadzącymi postępowanie dla celów ustalenia danych osób, które mogły dokonać zarzucanego czynu, np. udostępniając monitoring lokalu z daty, w której doszło do naruszenia.