Magdalena RYNKOWSKA

BEZPIECZEŃSTWO DANYCH OSOBOWYCH W CYBERPRZESTRZENI

STRESZCZENIE

Dane osobowe stanowią swoisty identyfikator osoby fizycznej. Na przestrzeni lat informacje będące dany osobowymi są stale zbierane i przetwarzane. Nieświadomość użytkowników w sieci prowadzi niejednokrotnie do kradzieży personaliów oraz wyłudzeń tożsamości. Poniżej przedstawiono sposób cyfrowego przetwarzania danych osobowych, a także anomalie społeczne, związane z kradzieżą personaliów oraz sposoby zapobiegania im w przyszłości.

Słowa kluczowe:
bezpieczeństwo danych osobowych, big data, przetwarzanie danych, scam, pushing, reklamy kierowane, wyłudzenia tożsamości

WSTĘP

Permanentny postęp technologii informacyjnych i komunikacyjnych, pozwala obecnie na pozyskiwanie dużej ilości informacji, których część stanowią dane osobowe. Proces gromadzenia, przetwarzania i analizy danych związany jest zarówno z sektorem prywatnym i publicznym. Informacje te są nie tylko cennym towarem dla funkcjonowania gospodarki, stanowią również atrakcyjny cel dla przestępców działających w sieci. Wyłudzenia tożsamości stały się powszechnym zjawiskiem, umożliwiającym oszustom na popełnianie szeregu innych przestępstw. W związku z tym, że świat wirtualny obecnie przenika do świata realnego, bardzo ciężko jest je czasami rozdzielić. Wynikiem tego jest fakt, że niestety przepisy prawa w zbyt małym stopniu są w stanie chronić osobę oraz jej informacje personalne. Ważne jest zatem uświadamianie społeczeństwa tj. prowadzenie kampanii informacyjnych i programów edukacyjnych, o możliwych zagrożeniach związanych z nieodpowiedzialnym korzystaniem z sieci.

OCHRONY DANYCH OSOBOWYCH - REGULACJE PRAWNE

Prawa w zakresie ochrony danych osobowych uregulowane są przede wszystkim w Konstytucji Rzeczypospolitej Polskiej[1], Ustawie o ochronie danych osobowych[2] oraz Rozporządzeniu MSWiA o przepisach wykonawczych do wcześniejszej ustawy[3], jednak problematyka ta dotyka również innych aktów prawnych związanych z działalnością gospodarczą, prawem pracy, bankowością telekomunikacją, rachunkowością i wieloma innymi.

Dane osobowe nie ograniczają się wyłącznie do podstawowych informacji takich jak imię i nazwisko, data i miejsce urodzenia, numer pesel czy NIP. Zgodnie z art. 6 ustawy z dnia 29 sierpnia 1997 r. za dane osobowe uważa się wszelkie personalia dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. W rozumieniu tego dokumentu osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, na podstawie jej cech fizycznych, fizjologicznych, umysłowych, ekonomicznych, kulturowych lub społecznych.[4] Definicja danych osobowych wraz z rozwojem technologii informatycznych dynamicznie się zmienia i przybiera różne formy.

Organem państwowym odpowiadającym za bezpieczeństwo danych osobowych jest Generalny Inspektor Ochrony Danych Osobowych (GIODO). Zgodnie z przepisami jest on uprawniony między innymi do:

- kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych;
- rozpatrywania skarg i wydawania decyzji w sprawach wykonania przepisów o ochronie danych osobowych;
- prowadzenia rejestrów zbiorów danych oraz administratorów bezpieczeństwa informacji;
- inicjowania i podejmowania przedsięwzięć w zakresie doskonalenia ochrony danych osobowych;

Administrator danych osobowych może dokonać ich przetwarzania w następstwie przesłanek określonych w Ustawie o ochronie danych osobowych, która stanowi, iż przetwarzanie ich jest dopuszczalne jeżeli:

- osoba, której dane dotyczą, **wyrazi na to zgodę,** chyba że chodzi o usunięcie dotyczących jej danych;

1 Tamże art. 47,51
2 Dz. U.1997 Nr 133 poz. 883
3 Dz. U. z 2004 Nr 100
4 Dz. U.1997 Nr 133 poz. 883 art. 6

- jest to **niezbędne** dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa;
- jest to **konieczne** do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to **niezbędne** do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą;
- jest **niezbędne** do wykonania określonych prawem zadań realizowanych dla dobra publicznego;
- jest to **niezbędne** dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

Wykorzystywanie i przetwarzanie danych osobowych bez zgody czy wiedzy, osoby której one dotyczą, jest działaniem nielegalnym, za co grozi odpowiedzialność karna. W przypadku stwierdzenia działania wyczerpującego znamiona przestępstwa określonego w ustawie, Generalny Inspektor kieruje do organu powołanego do ścigania przestępstw zawiadomienie o popełnieniu przestępstwa, dołączając dowody dokumentujące podejrzenie.[5] Niestety średni czas trwania postępowania od momentu złożenia skargi do GIODO, do wydania wyroku przez Naczelny Sąd Administracyjny jest bardzo długi, w roku 2015 wyniósł 1067 dni.[6]

W celu poprawy efektywności funkcjonowania w Polsce publicznoprawnej ochronie danych osobowych, od 25 maja 2018 roku zaczną obowiązywać przepisy europejskiego rozporządzenia o ochronie danych osobowych (RODO). Tym samym w Polsce pracuje się jednocześnie nad nowymi przepisami, które dotyczyć mają organów ochrony danych osobowych, postępowania prowadzonymi przed nimi oraz instytucjami odwoławczymi. Efektywność i skuteczność tych prac będzie można zatem oceniać w przyszłości.

BIG DATA

Z roku na rok ilość gromadzonych elektronicznych danych gwałtownie wzrasta, związane jest to przede wszystkim z rozwojem technologii informatycznych jak również z wciąż nowo powstającymi źródłami tych danych. Po raz pierwszy hasło „big data" pojawiło się pod koniec lat 90. ubiegłego wieku, panowie Michael Cox i David Ellsworth przedstawili problem związany ze zbiorem dużej ilości danych, które powodowały obciążenia pamięci głównej, dysku

[5] http://www.giodo.gov.pl/pl/537

[6] http://www.rp.pl/Opinie/301269962-ochrona-danych-osobowych-dlacego-niedziała.html

lokalnego.[7] W procesie Najprościej terminem tym określamy pozyskiwanie bardzo dużych ilości danychz różnego rodzaju źródeł, porównywanie ich ze sobą, następnie analizowanie i wyciąganie wniosków. Skutkiem przetwarzania danych jest budowanie profili między innymi osób fizycznych i przedsiębiorstw.[8]

W oparciu o możliwości technologiczne w dzisiejszych czasach dokonujemy cyfryzacji danych związanych z interesującymi, ważnymi i zabawnymi zdarzeniami naszego życia, niejednokrotnie publikując je później w sieci. Często używamy aparatu w tabletach i smarthphonach jako szybkiego notatnika do zapisu danych, których rejestracja nie koniecznie zawsze jest prawnie możliwa. Ilość gromadzonych i przetwarzanych danych jest tak ogromna, że śmiało można pokusić się o stwierdzenie, że Internet zalewany jest informacjami, aby lepiej zobrazować aktywność ludzi w sieci, poniżej przedstawiono rysunek charakteryzujący działania wybranych witryn i aplikacji zaledwie w przeciągu jednej minuty.

Należy w tym miejscu zwrócić uwagę na ilość danych otrzymywanych z mediów społecznościowych, gdzie to właśnie sami użytkownicy stanowią źródło milionów rejestracji i wpisów. Całe mnóstwo informacji w Internecie jest obecnie publicznie dostępnych lub stosunkowo łatwo można je zdobyć przy wykorzystaniu odpowiedniego oprogramowania. Problemu nie stanowią już metody, czy możliwości pozyskania i rejestracji danych ale sposoby znalezienia tak zróżnicowanych i złożonych algorytmów czy technologii, które umożliwiałyby wyodrębnienie informacji pozwalających na wykrycie wartościowej wiedzy.

[7] M. Cox i D.Ellsworth, *Application-Controlled Demand Paging for Out-of-Core Visualization,*1997

[8] Według prof. Jerzego Stefanowskiego z Instytutu Informatyki na Politechnice Poznańskiej specyfikę Big Data wyrażają definicje, wg. których Big Data są scharakteryzowane za pomocą wielu V: „High Volume (wielkość przetwarzanych danych), Variety (złożone, niejednorodne reprezentacje źródeł danych) Velocity (aspekt czasu przetwarzania, oraz problem zmienności danych wraz z upływem czasu), Veracity (gorsza jakość danych i pewność co do ich wartości niż w przypadku klasycznej analizy statystycznej). B. Marek *Ochrona danych osobowych w dobie Big Data – raport z konferencji,* Warszawa 2016.

Rys. 1. Ilość danych dostarczanych w czasie jednej minuty w sieci.

źródło: Opracowanie własne na podstawie GoGlobe

W dzisiejszych czasach big data ma ogromny wpływ na funkcjonowanie gospodarki, jednakże trzeba mieć na uwadze fakt, że nieodłącznie w sieci funkcjonuje również jednostka. Podstawą współpracy obywateli i przedsiębiorców powinno być zaufanie, dlatego też powinniśmy być w pełni świadomi tego z czym wiąże się publikacja informacji osobistych. Gromadzone dane nie powinny ingerować w intymność i wolność, które stanowią o prywatności każdego człowieka. Niestety często pomijanym aspektem jest brak informacji o tym, kto i w jaki sposób będzie te dane osobiste przetwarzał.

Reklamy kierowane są przykładem tego jak w big data, przetwarzane są dane osobowe dla celów biznesowych.

Reklamy kierowane

Istotna część działalności biznesowej dużych koncernów takich jak chociażby Google, Apple, Microsoft, Facebook i inne, opiera się w dużej mierze na wyświetlaniu reklam. Wyświetlanie ich zarówno w witrynach internetowych, usługach czy aplikacjach mobilnych zgodnie z polityką właścicieli daje użyt-

kownikom bezpłatny dostęp do wielu tych usług. Analiza ogromnej ilości danych pozwala na wybranie odpowiedniej reklamy artykułu czy usługi, tak aby ta była zgodna z preferencjami potencjalnego klienta i przykuwała jego uwagę.

Zgodnie z polityką prywatności np. Google wyświetla reklamy wytypowane na podstawie danych zebranych z urządzeń użytkowników, czyli informacje o: wyszukiwanych hasłach w przeglądarce, otwieranych stronach, oglądanych reklamach i filmach, kupowanych artykułach, używanych aplikacjach czy lokalizacji. Dodatkowo będąc zalogowanym na koncie webmaili do analizy przekazywane są również dane osobowe, takie jak imię, nazwisko, data urodzenia, przedział wiekowy, płeć i zainteresowania. [9]

Należy zauważyć, że rodzaj wybranych ustawień reklam oraz zalogowanie się będą miały wpływ na to ile informacji i jakie dane będą analizowane przez algorytmy. Przykładowo po zalogowaniu się na swoje konto pocztowe przez przeglądarkę WWW na służbowym komputerze i wyszukaniu stron dotyczących motoryzacji czy komputerów, na swoim prywatnym urządzeniu np. smartphonie tego samego dnia wyświetlać nam się będą reklamy z nowymi samochodami czy sprzętem komputerowym.

Reklamy wyświetlane na poczcie elektronicznej związane są z informacjami danego konta. Oznacza to, zalogowanie na konto przy korzystaniu z innych możliwości danego usługodawcy tj. wpisywanie haseł w wyszukiwarce, oglądanie filmów czy danych artykułów, może mieć wpływ na to jakie reklamy użytkownik widzi.

NIEZNANE SIECI WI-FI

Darmowe sieci Wi-Fi stały się wszechobecne, można z nich korzystać w kawiarniach, sklepach, hotelach, w wybranych punktach miasta, na dworcach czy lotniskach. Stanowią one bardzo duże udogodnienie w dzisiejszych czasach, kiedy trudno wyobrazić sobie funkcjonowanie na tabletach, laptopach i smartphonach nie będąc „online". Jednak nie wszyscy użytkownicy zdają sobie sprawę z tego, że publiczne i darmowe sieci rzadko kiedy są zabezpieczone taka jak te biurowe czy domowe.

Zagrożenie dla użytkowania otwartych sieci stanowią włamywacze, którzy wykorzystują oprogramowanie tupu sniffer (np. Wireshark, RawCap, tcpdump). Programy te przechwytują pakiety protokołów**,** dzięki czemu podglądacze mogą uzyskać dostęp do informacji na temat: przeglądanych stron, wysyłanych i odbieranych plików, konwersacji na komunikatorach czy danych dostępowych telnetu, następnie dane te mogą zapisać na swoim komputerze i wykorzystać nawet w późniejszym czasie. Rodzaje przechwytywanych pakie-

[9] www.support.google.com/adsence/answer/9713?hl=pl

tów zależeć będą od złożoności zastosowanego sniffera, programy mogą obserwować wszystkie kanały transmisyjne każdego segmentu. Tym samym nieszyfrowane hasła będą łatwo dostępne dla włamywacza. Sposób wyłapywania danych przez sniffera przedstawiono na rysunku poniżej.

Rys. 2. Zobrazowanie użycia sniffera w otwartym WiFi.
źródło: Opracowanie własne na podstawie www.thebestvpn.uk

Należy mieć na uwadze, że stosowanie programów pozwalających na podglądanie wysyłanych i odbieranych pakietów jest legalne w myśl wykorzystywania ich przez administratorów sieci do znalezienia i analizy problemów związanych z wydajnością lub niewydolnością łącza. Używanie snifferów do celów niezgodnych z ich przeznaczeniem wiąże się z karą określoną w art. 267 KK, czyli grzywną, karą ograniczenia albo pozbawienia wolności do lat dwóch.[10]

Oczywiście występowanie powyższych zagrożeń nie oznacza, że powinniśmy zaprzestać korzystania z darmowych hotspotów. Odpowiednie przygotowanie i przestrzeganie kilku podstawowych zasad umożliwi nam korzystanie z tych sieci w sposób bezpieczny. Przede wszystkim należy:

- unikać nieznanych sieci Wi-Fi, nie chronionych hasłem o podejrzanej nazwie;
- w urządzeniu wyłączyć opcję automatycznego łączenia się z sieciami bezprzewodowymi;

[10] Kodeks Karny art. 267 § 1-5.

- korzystać z bezpiecznych serwisów- takich, które stosują protokół SSL,
- korzystać z usług dostawców VPN;[11]
- używać programów antywirusowych i zapory.

Przestrzeganie powyższych zasad powinno w przyszłości zminimalizować ryzyko ataku na urządzenie użytkownika, niestety nie jest to złoty środek na wszystkie zagrożenia z jakimi możemy się spotka w sieci.

SCAM I PHISHING

Czym jest scam? Scam[12] może przybierać różne formy począwszy od wysyłania maili czy też tradycyjnych listów, przez użytkowanie usług internetowych po bezpośredni kontakt ofiary z oszustem. Zjawisko to charakteryzuje się wzbudzeniem zaufania, a następnie wykorzystania go do wyłudzenia pieniędzy, przedmiotów wartościowych ale również informacji osobistych. Fałszywa wiadomość może zarówno zawierać prośbę o pomoc dla ludzi dotkniętych nieszczęściem lub odnośniki do stron w celu odebrania pieniędzy z wygranej na loterii, w której nigdy nie braliśmy udziału. Poza pocztą elektroniczną coraz częściej zjawisko scamu występuje na portalach społecznościowych. Co dziennie można zaobserwować jak ludzie zamieszczają posty zawierające odnośniki do stron dotyczących lokalizacji bliskich, gwarantowanej nagrody, wysokich zysków czy rankingu najczęściej odwiedzanych osób[13]. Wysyłanie niebezpiecznych wiadomości poprzez aplikacje tzn. portali społecznościowych stanowi kuszącą alternatywę dla oszustów, ze względu na liczbę osób z nich korzystających, możliwości wysyłania wiadomości bez znajomości danej osoby i rozpowszechnianie jej w sposób niekontrolowany.

Ataki nazywane phishingiem[14] wiążą się z udostępnianiem przez ofiary takich danych jak: nazwa użytkownika (login), hasła, numery telefonów, daty urodzin, numery kart kredytowych itp. Phishing jest zjawiskiem, w którym oszuści masowo wysyłają wiadomości e-mail. Internetowi przestępcy przy zna-

[11] Virtual Private Network – jest to wirtualna sieć prywatna, do której dostęp jest moderowany i ograniczony. W VPN nie ma możliwości fizycznego połączenia wewnątrz jej, ponieważ jak wskazuje sama nazwa jest to sieć wirtualna. Stosowanie jej skutkuje zwiększeniem bezpieczeństwa sieci.

[12] Oksfordzki słownik angielsko-polski - scam z ang. – oszustwo, przekręt.

[13] Osoby korzystające z usług nieznanych aplikacji np. OverBlog - „*Kto mnie podgląda*" - często nie zdają sobie sprawy, że zgadzając się na warunki udostępniania dają aplikacji OverBlog swobodny dostęp do między innymi:. informacji o swoim profilu publicznym, adresie e-mail, dacie urodzin, listy znajomych, wydarzeń, lokalizacji, grup itp. Co więcej akceptacja warunków zezwala na publikację postów przez aplikację w imieniu właściciela konta umożliwiając tym samym znalezienie kolejnej nieświadomej osoby.

[14] K. Gorzelak, P. Jacewicz Biuletyn Bezpieczeństwa Komputerowego, 2011, s 1.

jomości usiłują nakłonić użytkownika do podjęcia działań zgodnych z ich oczekiwaniami. Jeszcze kilka lat temu terminem tym określano wyłącznie ataki związane z kradzieżą danych do logowania w bankach, obecnie dotyczy on niemal każdego przestępstwa dokonanego przez e-mail. Cyberprzestępcy korzystając z dostępnych możliwości w sposób profesjonalny przygotowują e-mail, tak by jak najbardziej przypominał on wiadomość od operatorów sieci, banków, sklepów internetowych czy znanych witryn. Celem tych ataków nie zawsze jest tylko wyłudzenie danych osobowych użytkownika, nierzadko wysyłane są wiadomości zawierające złośliwe odnośniki do stron lub załączniki, które mogą zainfekować komputer, powodując utratę kontroli nad urządzeniem.

Najczęstszymi metodami stosowanymi przez oszustów są:

- informowanie o dostępności aktualizacji sterowników na komputerze, po czym klikając w odnośnik na dysku instalowane jest złośliwe oprogramowanie;
- wiadomość o wygaśnięciu konta z prośbą o ponowne logowanie z podaniem nazwy użytkownika i hasła;
- informacja o zmianie statusu konta błędu podczas wylogowania lub problemie przy wykonanym przelewie, z prośbą o kliknięcie w adres odnośnika i zalogowaniu się w banku;
- informacja o możliwości śledzenia swoich bliskich, po czym następuje przekierowanie na stronę proszącą o podanie numeru telefonu swojego i drugiej osoby.

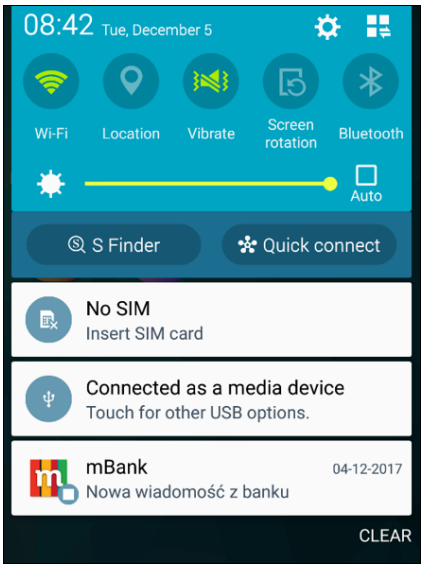
Powodzenie ataku zależy głównie od odbiorcy wiadomości, od użytkownika zależeć będzie czy pobrał dany załącznik, odpowiedział na e-mail czy wszedł na stronę znajdującą się w linku. W przypadku podejrzenia otrzymania wiadomości typu scam lub pushing najlepiej jest ją skasować. Należy być również wyczulonym na e-maile wymagające pilnego działania ze strony odbiorcy lub na takie, które wyglądają zbyt obiecująco. Używając kont pocztowych bez szyfrowania SSL musimy być również świadomi, że wysyłane e-maile mogą zostać przechwycone i przeczytane przez włamywacza. Kierowanie się zdrowym rozsądkiem pozwoli na bezpieczne korzystanie z poczty elektronicznej.

APLIKACJE MOBILNE

Łatwiejszy dostęp do informacji zapewniają nam również aplikacje mobilne, aktualnie spektrum ich wykorzystania jest nadzwyczaj szerokie. Posługujemy się nimi obecnie w praktycznie każdej strefie życiowej, umożliwiają nam one między innymi dostęp do gier, mediów społecznościowych, komunikatorów i poczty elektronicznej, pozwalają na przegląd informacji dotyczących po-

gody czy założonego planu treningowego, dokonywanie zakupów online, oglądania filmów VOD oraz wielu innych.

Mobilne aplikacje bankowe stanowią atrakcyjny cel dla cyberprzestępców, ponieważ dzięki nim mogą uzyskać bezpośredni dostęp do kont bankowych swoich ofiar. Pod koniec 2017 roku w Google Play pojawiły się co najmniej dwie aplikacje, których ściągnięcie i zainstalowanie na urządzeniu w wielu przypadkach skutkowało kradzieżą danych logowania do banku. StorySaver oraz CryptoMonitor teoretycznie miały służyć użytkownikom do innych celów, pierwsza z nich miała umożliwiać pobranie zdjęć i filmów z serwisu Instagram, druga natomiast monitorowanie kursów kryptowalut. Obydwie w rzeczywistości skanowały pamięć urządzenia, na którym zostały zainstalowane, w celu znalezienia dowolnej aplikacji bankowej. W przypadku, gdy aplikacja bankowa została znaleziona, użytkownik otrzymywał powiadomienie, przypominające prawdziwy komunikat bankowy, który prosił o zalogowanie się na fałszywej stronie .



Rys.3. Przykładowy komunikat z fałszywej aplikacji bankowej.
źródło: www.eset.pl

Dodatkowo instalacja aplikacji wiązała się z zezwoleniem na dostęp do skrzynki SMS, tym samym oszuści otrzymywali dane do logowania oraz możliwość przechwycenia kodów autoryzacyjnych. Po wykryciu złośliwych aplikacji ESET powiadomił Google o zagrożeniach, następnie aplikacje zostały usunięte.

Jednak do tego czasu jak wskazują eksperci zostały one pobrane kilka tysięcy razy przez polskich użytkowników.[15]

Nie dalej niż miesiąc później, na początku 2018 roku, doszło do kolejnych ataków na użytkowników bankowości mobilnej. Nowy typ kradzieży danych do kont bankowych dotyczył klientów mBanku. Jak przedstawiono w komunikacie na stronie banku ataki te przebiegały w kilku etapach[16]. W pierwszej kolejności oszuści pozyskiwali dane osobowe swoich ofiar, które umożliwiały im przejście poprawnej weryfikacji w rozmowie z operatorem sieci. Podczas konsultacji z operatorem podszywając się pod klienta dokonywali przekierowania połączeń z numeru ofiary na swój numer telefonu. Następnie przestępcy mogli dokonać sparowania konta klienta z aplikacją mobilną na urządzeniu, wykorzystywali do tego wcześniej uzyskane dane osobowe oraz przechwycone kody autoryzacyjne, które trafiały do nich po włączonej usłudze przekierowania połączeń u operatora. W ten sposób złodzieje dokonywali kradzieży z kont bankowych przelewając środki pieniężne zgodnie z limitami na koncie. Skala problemu oraz ilości skradzionych tą metodą pieniędzy nie jest znana. Bank natomiast na swojej stronie internetowej stara się uświadomić swoich klientów o zagrożeniach oraz sposobach obrony przed takimi atakami.

Możliwości jakie niesie za sobą używanie aplikacji mobilnych są olbrzymie, można powiedzieć, że dają one nieograniczony dostęp do informacji. Należy jednak mieć na uwadze zagrożenia jakie mogą pojawić się w przypadku nierozsądnego ich używania. Podobnie jak w przypadku wiadomości scam czy phishing , zawsze powinno się sprawdzać wiarygodność i źródło pochodzenia danej aplikacji, blokować pozwolenie na dostęp do naszych prywatnych danych lub innych programów, które wydają się nie być potrzebne do funkcjonowania danej aplikacji, a także posiadać program antywirusowy na swoim urządzeniu. Zastosowanie się do tych rad może pomóc w przyszłości uniknąć ataku cyberprzestępców.

WYŁUDZENIA TOŻSAMOŚCI SKALA PROBLEMU

Jak opisano już wcześniej ilość przetwarzanych obecnie danych osobowych jest ogromna, w każdej sekundzie w kontekście big data do centrów obliczeniowych docierają terabajty danych. Codziennie każdy może stać się potencjalną ofiarą zagrożeń jakie niesie ze sobą korzystanie z dobrodziejstw technologii, nowych aplikacji czy dostępu do sieci. Nie zawsze skutkiem wyłu-

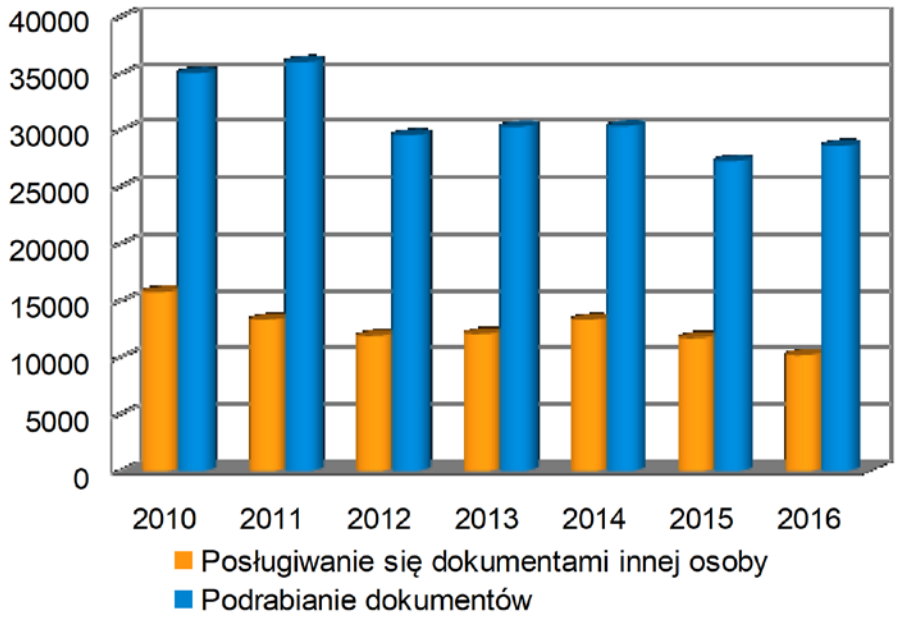
[15] Zgodnie z informacjami ekspertów z ESET aplikacje te mogły podszywać się pod powiadomienia nawet czternastu banków, a ponad 96% wykrytych przypadków zagrożenia zainfekowanymi programami pochodzi z Polski. Źródło: www.eset.pl

[16] Źródło: www.mbank.pl/informacje-dla-klienta/indywidualny

dzeń danych osobowych są korzyści majątkowe, przynajmniej nie na pierwszy rzut oka. Gdy w mediach słyszy się o kolejnych atakach na bazy danych w dużych firmach, zazwyczaj nie przykuwa się do tego większej wagi. Problem ten jednak istnieje i dotyczy bardzo wielu ludzi. Przykładowo w 2016 roku hakerzy włamali się do baz danych Ubera i wykradli z nich informacje o 57 milionach użytkowników z całego świata. Bazy te zawierały dane zarówno o kierowcach jak i klientach firmy, wykradzione informacje dotyczyły: nazwisk, numerów telefonów, adresów e-mail, a także numerów praw jazdy, o wszystkim poinformował nowy szef firmy, rok po zdarzeniu. Tego samego roku z serwerów portalu mail.ru, z których skradziono dane z 64 milionów kont. Hakerzy wykradli również około 40 milionów haseł klientów Yahoo, 33 miliony z Hotmail i 24 miliony haseł Gmail. Sumując, spowodowało to zagrożenie dla ponad 272 milionów kont e-mail.[17] Z kolei w październiku 2017 roku operator telekomunikacyjny T-Mobile wykrył kradzież danych swoich klientów. W zorganizowaną akcję zaangażowani byli pracownicy call center oraz firmy marketingowej, którzy jak się później okazało poprzez nieuprawniony posiadali dostęp do bazy danych przetwarzać informację zawierające dane abonentów i przekazywać je operatorowi konkurencyjnemu. Problem został wykryty przez system bezpieczeństwa, dzięki czemu sprawców złapano. T-Mobile złożył zawiadomienie do prokuratury oraz GIODO zatrzymanym przedstawiono zarzuty z artykułów 266 KK, 267 KK, 269b KK oraz art. 49.

Kradzież cyfrowych danych osobowych powoduje, że przestępcy nie muszą uciekać się tylko i wyłącznie do metod rabunku będąc w bezpośrednim kontakcie z ofiarą. Tym samym do wyłudzenia pieniędzy np. w bankach nie ma potrzeby przedstawiania się dowodem osobistym, można to zrobić logując się na konto bankowe i wykonując odpowiedni przelew.

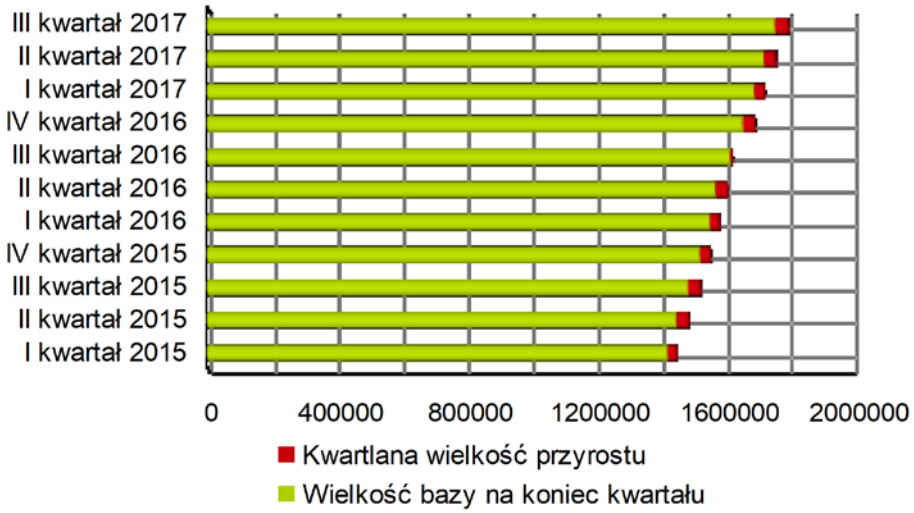
[17] http://di.com.pl/kradziez-danych-instagrama-najlepszym-przykladem-jak-latwo-mozna-stracic-prywatnosc-58182



Rys. 4. Charakterystyka zmian dotyczących dokumentów osobistych.

źródło: Opracowanie własne na podstawie infoDOK 2017

Wykres zawiera informacje pochodzące z Kampanii Informacyjnej Systemu Dokumentów Zastrzeżonych. Zgodnie z przedstawionymi danymi na przestrzeni ostatnich pięciu lat dziennie dochodzi do podrobienia ponad siedemdziesięciu dokumentów osobistych, co więcej około trzydziestu osób posługuje się dokumentami innej osoby. Wyłudzenia danych skutkują wzrostem liczby zastrzeganych dokumentów tożsamości, co przedstawiono na kolejnym wykresie.



Rys. 5. Charakterystyka kwartalnego przyrostu danych do bazy dokumentów zastrzeżonych.

źródło: Opracowanie własne na podstawie infoDOK 2017

Jak wynika z przedstawionych danych ilość zastrzeganych dokumentów, stale rośnie. W wyniku kradzież danych osobowych, w tym również informacji z kart płatniczych czy danych do logowania na konta bankowe pod koniec II kwartału 2017 roku dokonano prób wyłudzeń kredytów na łączną kwotę prawie 205 mld złotych.

Podane informacje ukazują skalę problemu związanego z kradzieżą danych osobowych. W czasach kiedy świat wirtualny przenika do świata realnego, obywatele narażeni są nie tylko na kradzież fizycznych dokumentów osobowych ale również na wyłudzenie cyfrowych danych przez oszustów, które podobnie jak te pierwsze mogą być narzędziem pozwalającym na przywłaszczenie sobie dóbr osobistych ofiary.

WNIOSKI

Wraz z rozwojem możliwości technologicznych i informatycznych zachowanie bezpieczeństwa danych osobowych w cyberprzestrzeni staje się trudne do utrzymania. Gromadzenie informacji personalnych jest coraz prostsze, szczególnie wobec osób bardzo aktywnych w mediach społecznościowych. Codzienne możliwości i udogodnienia jakimi kuszą użytkowników otwarte sieci WiFi, portale społecznościowe, aplikacje mobilne i inne często powodują, że nieświadomie narażamy siebie na niebezpieczeństwa ze strony hakerów i oszustów. Tylko świadome korzystanie z dobrodziejstw sieci może pozwolić

na uniknięcie lub przynajmniej zminimalizowanie skutków ataków przeprowadzanych przez cyberprzestępców.

BIBLIOGRAFIA

[1] Burzyński M., *Szanse i zagrożenia rozwoju koncepcji Big Data na przykładzie sektora publicznego*, 2014.

[2] Cox M. i Ellsworth D*., Application-Controlled Demand Paging for Out-of-Core Visualization,*1997.

[3] Federal Bureau of Investigation, *2015 Internet Crime Report*, U.S. Departmet of Justice, 2015.

[4] K. Gorzelak, P. Jacewicz Biuletyn Bezpieczeństwa Komputerowego, 2011, s 1.

[5] Janus R., C*o widać w niezabezpieczonej sieci WiFi?*, ITfoucus 2009.

[6] Kondek G. i Ożarowska E., *infoDOK – raport o dokumentach*, wyd. 31, 2017.

[7] Marek B., *Ochrona danych osobowych w dobie Big Data* , Warszawa, 2016.

[8] The SANS Institute, *OUCH! - Biuletyn Bezpieczeństwa Komputerowego*, Cert Polska, 2011.

[9] Ustawa z dnia 1997 o ochronie danych osobowych (Dz. U. 1997 Nr 171, poz 81800 z późn. zm.)

[10] Ustawa z dnia 16 lipca 2004r. Prawo telekomunikacyjne (Dz. U. 1997 Nr 133, poz 883)

[11] www.di.com.pl

[12] www.eset.pl

[13] www.giodo.gov.pl

[14] www.mbank.pl

[15] www.rp.pl

[16] www.thebestvpn.uk

SECURITY OF PERSONAL DATA IN CYBERSPACE

ABSTRACT

Personal data is a specific identifier of a natural person. Over the years, personal information is constantly collected and processed. The article treats about method of digitally processing personal data, as well as social anomalies such as: theft of personal data or identity frauds and ways to prevent them in the future.