9 zagrożeń

dla bezpieczeństwa danych osobowych

experto24.pl

Spis treści

Na administratorach danych ciąży obowiązek zapewnienia bezpieczeństwa systemów teleinformatycznych. Obszar ten bardzo często jest zaniedbywany bądź pomijany. W związku z tym warto wprowadzić mechanizmy, które pomogą zmniejszyć ryzyko wystąpienia incydentu. Dobrze jest np. opracować procedurę reagowania na incydenty, które wraz z rozpoczęciem obowiązywania ogólnego rozporządzenia o ochronie danych (RODO) i tak będą obligatoryjną procedurą na podstawie art. 33 i 34 RODO. W procedurze tej należy określić, w jakich sytuacjach ma ona umożliwić minimalizację szkód. W przypadku wystąpienia określonego incydentu powinna wskazywać natomiast, co pracownik powinien zrobić, by zabezpieczyć miejsce zdarzenia oraz minimalizować powstałe szkody, a także kogo poinformować o incydencie. Ponadto po przeanalizowaniu przyczyn i skutków zdarzenia powodującego naruszenie bezpieczeństwa przetwarzanych danych osobowych, osoby odpowiedzialne za bezpieczeństwo danych osobowych zobowiązane są podjąć wszelkie inne działania mające na celu wyeliminowanie podobnych naruszeń w przyszłości oraz zmniejszenie ryzyka występowania ich negatywnych skutków. Poznaj 9 najczęstszych zagrożeń dla bezpieczeństwa danych osobowych.

1. Pliki cookies

Pliki cookies, czyli popularne „ciasteczka”, zostały stworzone, aby ułatwić weryfikację użytkownika korzystającego z wybranej strony internetowej. Poprzez umieszczenie plików cookies na komputerze użytkownika możliwe jest uzyskanie informacji na temat tej osoby, jej hasła, adresu e-mail, ale także jego preferencji na podstawie dokonywanych przez niego wyborów. Celem plików cookies staje się stworzenie jak najbardziej zindywidualizowanej i interesującej dla użytkownika usługi bądź oferty. Za ich pośrednictwem możliwe jest poznanie gustu, upodobań użytkownika lub przeciwnie –

wyeliminowanie usług bądź produktów, które go nie interesują. W związku z tym w ocenie wielu osób są to narzędzia, które w nadmierny sposób ingerują w prywatność użytkowników. W ocenie innych ekspertów nie wszystkie pliki cookies stanowią zagrożenie dla prywatności jednostki, sam w sobie plik cookies nie zawiera bowiem informacji identyfikującej użytkownika. Jednak czy interesowanie się tym, jakie książki czytamy, jakiej muzyki słuchamy, jakie są nasze gusta kulinarne, nie stanowi ingerencji w prywatność jednostki? Informacje te mają kluczowe znaczenie dla przedsiębiorców w momencie oferowania użytkownikowi określonej usługi lub towarów. Dane te są więc dla wielu podmiotów cennym źródłem informacji, za które gotowe będą zapłacić każdą sumę pieniędzy, a przecież w społeczeństwie informacyjnym informacja jest dobrem równie cennym jak pieniądz.

Dlatego też na każdej odwiedzanej przez użytkownika stronie internetowej powinny pojawiać się informacje na temat wykorzystywania plików cookies. Obowiązek ich umieszczania wynika z art. 173 Prawa telekomunikacyjnego. W związku z tym od 22 marca 2013 r. każdy administrator strony internetowej jest zobowiązany poinformować użytkownika o wykorzystywaniu plików cookies. Obowiązujące przepisy wymagają również uzyskania od niego zgody na zapisanie ich na jego twardym dysku. Zgodnie z art. 173 Prawa telekomunikacyjnego „przechowywanie informacji lub uzyskanie dostępu do informacji już przechowywanej w telekomunikacyjnym urządzeniu końcowym abonenta lub użytkownika końcowego jest dozwolone, pod warunkiem że abonent lub użytkownik końcowy po otrzymaniu informacji, o których mowa w pkt 1 cyt. artykułu, wyrazi na to zgodę". Problem jednak w tym, że większość przeglądarek ma fabryczne ustawienie akceptujące pliki cookies, co uniemożliwia użytkownikowi podjęcie dobrowolnej i świadomej zgody, tak jak wymagają tego przepisy. Podstawowym celem wprowadzenia plików cookies było podniesienie jakości świadczonych usług, tymczasem można odnieść wrażenie, że szeroko rozumiane prawa, w tym prawo do prywatności użytkownika, pełnią rolę drugorzędną, bardzo często nie jest on bowiem świadomy przysługujących mu praw.

Chociaż dostępne rozwiązania technologiczne umożliwiają blokowanie bądź usuwanie plików cookies, wielu użytkowników nie jest tego świadoma. Dodatkowo wielu z nas nie zastanawia się nad konsekwencjami związanymi z obecnością plików cookies i dla świętego spokoju akceptuje warunki oferowane przez administratorów.

Niewłaściwą, choć spotykaną praktyką, jest uzależnianie możliwości korzystania ze strony internetowej od zgody użytkownika na wykorzystywanie plików cookies.

2. Kradzież tożsamości

Słowo „tożsamość" – łac. *identicus* – oznacza: taki sam, ten sam, jednakowy. Pojęcie to coraz częściej używane jest na określenie przestępstwa polegającego na podszywaniu się pod inną osobę i wykorzystywaniu jej wizerunku lub innych jej danych osobowych w celu wyrządzenia jej szkody majątkowej lub osobistej (art. 190a § 2 Kodeksu karnego – kk).

Jak zauważył Wojewódzki Sąd Administracyjny w Warszawie w wyroku z 3 marca 2009 r. (sygn. akt II Sa/Wa 1495/08), „w języku polskim pojęcie tożsamości oznacza cechy, które stanowią o tym, kim dana osoba jest, czym się różni od innych. Na tak rozumianą tożsamość składa się nie tylko to, kim się jest obecnie, ale również to, kim się było, a nawet zamierzenia na przyszłość, wszystko to, co powoduje, że dana osoba różni się od innej". Warto zwrócić uwagę, że o ile samo podszywanie się pod inną osobę nie jest karalne, o tyle jednak robienie tego w celu uzyskania określonej korzyści już tak.

Pojęcie „kradzieży tożsamości" pojawia się w wielu aktach prawnych zarówno krajowych, jak i międzynarodowych. Pionierem w tym zakresie były Stany Zjednoczone, a pierwsze regulacje powstały w 1996 roku. W związku z dynamicznym rozwojem kradzieży tożsamości międzynarodowe organizacje rządowe (w tym ONZ) podjęły działania mające na celu ograniczenie tego zjawiska. W jednym z dokumentów ONZ podkreślono, że kradzież tożsamości powinna być karana na tyle surowo, aby być traktowana jako poważne przestępstwo w rozumieniu wspomnianej konwencji przeciwko międzynarodowej przestępczości zorganizowanej. Za poważne przestępstwo są przy tym uważane czyny, które są zagrożone karą o górnej granicy, co najmniej 4 lat pozbawienia wolności lub karą surowszą. Znacznie później zaczęto dostrzegać zagrożenie kradzieży tożsamości w Unii Europejskiej. Wyraźnym impulsem stał się komunikat Komisji Wspólnot Europejskich z 22 sierpnia 2007 r., w którym zdefiniowano kradzież tożsamości jako wykorzystanie identyfikujących danych personalnych, na przykład numeru karty kredytowej jako narzędzia do popełnienia innych przestępstw. Warto zauważyć, że na gruncie prawa europejskiego nie ma wiążącego aktu prawnego, kompleksowo odnoszącego się do tego przestępstwa. W związku z tym ciężar odpowiedzialności został przeniesiony na państwa członkowskie, czego najlepszym przykładem jest art. 190a § 2 kk, który umieszcza je w rozdziale dotyczącym przestępstw przeciwko wolności.

Tymczasem okazuje się, że zjawisko to może mieć charakter globalny i wykraczać poza jurysdykcję jednego państwa. Warto więc zastanowić się nad wypracowaniem wspólnych wytycznych w tym obszarze. Znamion tego przestępstwa nie będzie wypełniać podszywanie się pod osobę nieistniejącą, wymyśloną. Przedmiotem kradzieży mogą być różne dane: od tożsamości osoby fizycznej, po hasła dostępu do konta bankowego, nick, hasło dostępu do portalu społecznościowego czy PESEL.

Chociaż kradzież tożsamości nie jest zjawiskiem nowym, od pewnego czasu obserwujemy rozwój tego przestępstwa. Coraz częściej słyszymy o wyciekach danych z baz danych na dużą skalę: numerów PESEL, haseł dostępu, numerów kart bankowych lub innych informacji służących do popełnienia przestępstwa. Główną przyczyną wzrostu odnotowań kradzieży tożsamości jest niewątpliwie rozwój Internetu, za którego pośrednictwem rozwija się handel elektroniczny, bankowość elektroniczna czy portale społecznościowe. Stał się on impulsem do kradzieży tożsamości na większą niż do tej pory skalę. Wynika to przede wszystkim z tego, że w celu ustalenia tożsamości osoby fizycznej nie jest wymagane jej dodatkowe potwierdzenie. Ponadto warto uświadomić sobie, że w czasach, gdy informacja stanowi dobro równie cenne jak pieniądz, wymiana informacji (również na temat jednostki) odbywa się na niebywałą dotychczas skalę. Dane na temat stanu zdrowia pacjenta są tak cenne, że

korporacje międzynarodowe gotowe są zapłacić za nie niemal każdą kwotę, a w przypadku wycieku danych wrażliwych okupy za nie przybierają niewyobrażalne kwoty.

Wśród najczęściej stosowanych metod przez sprawców kradzieży tożsamości w sieci, są *phishing*, *pharming* czy też użycie oprogramowania szpiegującego. Często bowiem kradzież tożsamości jest połączona z innego rodzaju przestępstwem. Zjawisko to jest niebezpieczne nie tylko dla ofiary przestępstwa, ale również dla gospodarki, gdyż oprócz wyrządzenia bezpośrednich szkód majątkowych osłabia zaufanie do handlu elektronicznego, elektronicznych instrumentów płatniczych i innych usług.

W praktyce okazuje się, że znacznie lepiej chronimy dane osobowe w rzeczywistości niż w Internecie. Wydaje się, że powodem takiego stanu rzeczy jest przekonanie, że są nikłe szanse, by przestępca zainteresował się naszymi danymi. Ponadto w wirtualnym świecie pojęcie „przestępca" nabiera bardziej abstrakcyjnego charakteru, dlatego też rzadziej wzbudza w nas strach.

Bardzo często do kradzieży tożsamości dochodzi poprzez tworzenie fałszywej strony internetowej łudząco podobnej do oryginalnej i pozyskanie w ten sposób danych użytkownika czy też podszywanie się pod znane marki i wysyłanie nieprawdziwych wiadomości e-mail rzekomo z banków czy innych usługodawców, zmuszających podmiot do przekazania danych osobowych.

Zazwyczaj najbardziej dotkliwie skutki kradzieży tożsamości odczuwa pokrzywdzony, zwłaszcza gdy przestępstwo to jest powiązane z przestępstwami przeciwko mieniu, a pokrzywdzony ponosi szkodę majątkową. Niestety większość z nas o kradzieży tożsamości dowiaduje się dopiero po roku. W związku z tym – w znaczący sposób zostaje ograniczona możliwość przeciwdziałania skutkom kradzieży. Niemniej jednak warto pamiętać, by mimo to możliwie szybko zgłosić kradzież dokumentu tożsamości czy utratę środków finansowych na koncie. Kradzież tożsamości może wiązać się z ryzykiem wystąpienia także innych konsekwencji. Przede wszystkim może niekorzystnie wpłynąć na poczucie pewności i zaufania pokrzywdzonych, zwiększyć ich strach, stres czy nawet przyczynić się do rozwoju agresji.

Warto wskazać, że czynności wskazane w art. 190a § 2 kk zagrożone są karą pozbawienia wolności od 1 miesiąca do lat 3. Oznacza to, że wobec sprawców tych czynów możliwe jest zastosowanie instytucji warunkowego umorzenia postępowania karnego.

3. Phishing

Phishing to atak, który polega na wyłudzeniu danych użytkownika, takich jak jego nazwa (login), hasło czy numer konta poprzez tworzenie fałszywych witryn internetowych łudząco podobnych do stron internetowych znanych nam podmiotów.

Typowy atak phishingowy polega na wysłaniu e-maila zawierającego fałszywe linki, które kierują użytkownika na odpowiednio opracowane strony. Strona taka przechwytuje następnie informacje wpisywane przez nieświadomych użytkowników w formularzach, które następnie są wykorzystywane przez przestępców.

4. Pharming

Najbardziej zaawansowaną i trudną do wykrycia odmianą *phishingu* jest *pharming*. Atak polega na tym, że przestępca instaluje na komputerze użytkownika złośliwe oprogramowanie, które modyfikuje wpisy w pliku „host" lub „lmhosts". System operacyjny wykorzystuje następnie właśnie te pliki do przechowywania informacji o odwzorowaniach nazw symbolicznych na adresy IP i są one sprawdzane w pierwszej kolejności, zanim system wyśle zapytanie do serwera.

5. Złośliwe oprogramowanie

Złośliwe oprogramowania są instalowane na komputerach użytkowników bez ich wiedzy. Za ich pośrednictwem możliwe jest nie tylko kontrolowanie komputera użytkownika, ale także przejęcie nad nimi pełnej władzy i doprowadzenie do kradzieży danych. Podobnie jak w przypadku innych zagrożeń, także w tym obszarze w ostatnich latach odnotowuje się wzrost. Jeżeli administrator danych nie korzysta z legalnych programów antywirusowych, z łatwością naraża się na naruszenie. Warto także stosować kilka reguł wynikających z dobrych praktyk, np. nie otwierać e-maili nieznanego pochodzenia, nie podłączać pod swój komputer nośników obcego pochodzenia.

6. Wirusy

Są to programy komputerowe, których funkcja sprowadza się do zakłócenia pracy komputera poprzez uszkodzenie lub niszczenie danych. W celu ochrony komputerów przed wirusami instalowane są programy antywirusowe, które je blokują. Najczęściej wirusy są przenoszone przez wiadomości e-mail, przenośne nośniki, pliki PDF. Ich obecność może przyczynić się nie tylko do spowolnienia pracy komputera, ale także utraty danych. Administrator danych powinien zadbać, by program antywirusowy był instalowany nie tylko na komputerach stacjonarnych pracowników, ale także laptopach, tabletach czy smartfonach. Informacje na temat stosowanych programów, a także częstotliwość ich aktualizacji oraz instrukcja, w jaki sposób powinien zachować się pracownik w przypadku wykrycia wirusa, powinna znaleźć odzwierciedlenie w instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

7. Robaki

To odmiana szkodliwego programu komputerowego, który rozprzestrzenia się samodzielnie, obciążając pamięć komputera. Często obecność tego typu wirusa poza utratą danych może doprowadzić do samoczynnego wysyłania wiadomości czy przekierować użytkownika na nieznane mu strony. Wirus ten ma także zdolność szybkiego rozprzestrzeniania się na komputerze użytkownika. To zaś stanowi poważne zagrożenie dla ochrony danych osobowych przetwarzanych przez użytkownika.

8. Konie trojańskie

To kolejny przykład złośliwego oprogramowania, które może przyczynić się do utraty danych i naruszyć bezpieczeństwo systemu teleinformatycznego w jednostce organizacyjnej. W przeciwieństwie do robaków konie trojańskie nie są w stanie same się rozprzestrzeniać. Bardzo często konie trojańskie są wykorzystywane do pozyskiwania danych finansowych, w tym numerów rachunków bankowych, loginów, haseł.

9. Spam

Każdy z nas na skrzynkę e-mail otrzymuje setki wiadomości nieznanego pochodzenia. Najczęściej są to reklamy oferujące nowy produkt bądź oferta pożyczki na atrakcyjnych warunkach, oferta handlowa lub zaproszenie do wzięcia udziału w grze. Bardzo często już sam temat wiadomości jest zatytułowany w taki sposób, by zachęcić użytkownika do jej otwarcia. W tej postaci informacje trafiają do milionów nieznanych adresatów. W przeważającej większości przypadków jest to niezamówiona informacja, nikt nie pyta bowiem użytkownika, czy chce ją otrzymać. Otwarcie poczty od niezidentyfikowanego nadawcy stanowi zagrożenie, że zostanie aktywowane złośliwe oprogramowanie. Spam może także powodować blokowanie miejsca na twardym dysku. Dostrzegając te zagrożenia, polski ustawodawca krytycznie ustosunkował się do tego typu praktyk. Zgodnie z art. 10 ustawy o świadczeniu usług drogą elektroniczną „zabronione jest przesyłanie niezamówionej informacji handlowej skierowanej do oznaczonego odbiorcy będącego osobą fizyczną za pomocą środków komunikacji elektronicznej, w szczególności poczty elektronicznej". Chociaż istnieją przepisy ograniczające możliwość wysyłania spamu, w praktyce nie są ani przestrzegane, ani egzekwowane. W związku z tym warto samemu zadbać o swoje bezpieczeństwo, m.in. poprzez założenie filtru antyspamowego, który odseparuje wiadomości spam tak, by nie zaśmiecały nam skrzynki.

Autor:
Agnieszka Stępień

Stopka redakcyjna

Redaktor:	Wioleta Szczygielska
ISBN:	978-83-269-6914-0
E-book nr:	2HH0648
Wydawnictwo:	Wydawnictwo Wiedza i Praktyka sp. z o.o.
Adres:	03-918 Warszawa, ul. Łotewska 9a
Kontakt:	Telefon 22 518 29 29, faks 22 617 60 10, e-mail: *cok@wip.pl*
NIP:	526-19-92-256
Numer KRS:	0000098264 – Sąd Rejonowy dla m.st. Warszawy, Sąd Gospodarczy XIII Wydział Gospodarczy Rejestrowy. Wysokość kapitału zakładowego: 200.000 zł