

RAPORT

CERT POLSKA



Zabezpieczenie prywatności w usługach internetowych

na przykładzie

dostawców „darmowych kont poczty elektronicznej”

Andrzej Chrzęszcz, Mirosław Maj

CERT POLSKA

cert@cert.pl

Spis treści

Spis treści	2
1. Wstęp.....	3
2. Zbieranie danych osobowych przez Internet.....	3
3. Kto pozyskuje dane osobowe?	3
4. Jakie są zagrożenia?	5
5. Kryteria oceny ochrony danych	6
5.1 Zagadnienia formalno – organizacyjne	6
5.2 Zakres pozyskiwania i przetwarzania danych osobowych.....	7
5.3 Techniczne sposoby zabezpieczania danych osobowych	7
6. Badanie CERT POLSKA	8
7. Metodologia badania	8
8. Wyniki badania	9
8.1 Kryteria formalno – organizacyjne	9
8.1.1 Regulamin	9
8.1.2 Ochrona prywatności.....	10
8.1.3 Prawo do poprawiania.....	10
8.1.4 Usunięcie danych osobowych	11
8.1.5 Brak zobowiązania poprawności danych osobowych.....	11
8.2 Cel przetwarzania danych osobowych	12
8.3 Zakres zbierania danych.....	12
8.4 Kryterium techniczne	13
8.4.1 Zróżnicowanie loginu i hasła użytkownika serwisu	13
8.4.2 Minimalna długość hasła.....	14
8.4.3 Znaki specjalne w hasle.....	14
8.4.4 Możliwość zmiany hasła	15
8.4.5 Szyfrowanie.....	15
9. Zbiorcze zestawienie wyników badań.....	15
10. Wnioski	16
11. Propozycja zakresu wymagań	17
11.1 Kryteria formalno – organizacyjne	18
11.2 Kryteria techniczne	18
12. Literatura	20

1. Wstęp

Niniejszy raport ma na celu przedstawienie w podstawowym zarysie problematyki ochrony danych osobowych osób korzystających z usługi darmowej poczty elektronicznej.

Możliwość założenia konta poczty elektronicznej stała się jedną z podstawowych usług, jakie oferują właściciele dużych portali internetowych. Niewątpliwie opcja ta ma za zadanie spopularyzować dany portal, wśród internautów, co w rezultacie daje właścicielowi portalu lepszą pozycję w rozmowach z potencjalnymi i posiadany już reklamodawcami. Nie jest również tajemnicą, że w zamian za możliwość korzystania z usług serwerów administratorów portali, klient jest zazwyczaj zmuszany do przekazania swoich danych osobowych, oczywiście wraz ze zgodą na ich przetwarzanie. Powstaje więc pytanie, jakie dane przekazujemy danemu administratorowi i co dalej za tym idzie – jak one są chronione.

2. Zbieranie danych osobowych przez Internet

Od pewnego czasu, także w Polsce, wszelkiego rodzaju informacja stała się niewątpliwie cennym towarem. Dotyczy to również danych osobowych. W warunkach gospodarki wolnorynkowej, w której znacznie większy problem stanowi znalezienie klienta niż towaru, właśnie dane osobowe, umożliwiające dotarcie do potencjalnych klientów stały się bardzo cenne. Oczywiście w takiej sytuacji powstaje problem sposobu ich pozyskiwania. Wraz z rozwojem Internetu zauważono, że pozyskiwanie danych osobowych, właśnie przez Internet, jest bardzo tanie i stosunkowo skuteczne. Dlatego dziś niezwykle powszechne stały się takie miejsca w Internecie gdzie w zamian za mniejszą lub większą usługę pozyskuje się dane osobowe korzystającego z usługi.

3. Kto pozyskuje dane osobowe?

Najłatwiej można by rzec, że wszyscy. Stwierdzenie takie nie miałyby się daleko z prawdą. Aby się o tym przekonać, przeprowadziliśmy proste doświadczenie, które polegało na wpisaniu do jednej z popularnych polskich wyszukiwarek internetowych, formuły „Zgadzam się na przetwarzanie moich danych osobowych” wychodząc z założenia, że tak brzmiąca formuła towarzyszy niemalże wszystkim

przypadkom prób formalnego i zgodnego z prawem pozyskania danych osobowych. Nasze przypuszczenia się potwierdziły i tak, dla przykładu, przedstawiamy poniżej tylko kilka z pierwszych pozycji listy prezentującej wyniki poszukiwania:

- Firma leasingowa, oferując w zamian za dane osobowe możliwość zapoznania się z ofertą dotyczącą unikalnej, limitowanej wersji samochodu;
- Niewielka firma handlowa sprzedająca oprogramowanie, firma ta przy okazji zamówienia zbierała dane, których zakres zdecydowanie przekraczał zestaw danych koniecznych do wywiązania się z umowy;
- Firma sprzedająca bilety do kina, zbierająca dane o zamawiającym w celu wysłania potwierdzenia rejestracji, prosiła o podanie informacji, których zakres wydawał się szerszy niż konieczny do dokonania takiego potwierdzenia;
- Jeden z większych producentów sprzętu RTV w kwestionariuszu na swojej stronie prosił o imię, nazwisko, adres, telefon, zawód, adres poczty elektronicznej, wiek i płeć, oferując w zamian możliwość zagrania w wirtualne...puzzle (gra trwała około 30 sekund)

Wśród wszystkich „kolekcjonerów danych osobowych” można wyróżnić pewne ich kategorie. Rozróżnienia takiego można dokonać na przykład w oparciu o oferowaną przez nich usługę (w zamian, za którą pozyskują oni dane osób z niej korzystających). Niewątpliwie jedną z wyodrębnionych według takiego klucza kategorii, stanowią oferenci darmowych kont pocztowych.

Właśnie w oparciu o tę kategorię chcielibyśmy ocenić zakres pozyskiwania danych jak również stosowane mechanizmy ich ochrony. Czy rzeczywiście konta te są darmowe? Biorąc pod uwagę to, co stwierdziliśmy wcześniej, a mianowicie fakt, że informacja jest dziś nie mniej cennym towarem niż dobra materialne, to trzeba sobie jasno odpowiedzieć, że konta te nie są darmowe. Warto więc zrobić rozeznanie ile tak naprawdę żądają od nas usługodawcy za oferowaną usługę i dodatkowo, co jest niezwykle ważne, jak chronią powierzone im dane. Poprzez dane te rozumiemy nie tylko standardowe dane osobowe, takie jak: imię, nazwisko czy adres zamieszkania, itd., ale również te dane, które stanowią istotną osobistą informację, czyli krótko mówiąc, w tym wypadku, treść naszej prywatnej korespondencji.

4. Jakie są zagrożenia?

Zanim dokonamy oceny poziomu bezpieczeństwa danych osobowych u dostawcy kont pocztowych, zatrzymajmy się na chwilę przy zagrożeniach związanych z danymi osobowymi w Internecie. Są one zasadniczo podobne do zagrożeń, na jakie narażone są wszelkiego typu dane przechowywane, udostępniane czy przesyłane przez sieci rozległe. Niemniej jednak warto usystematyzować tę wiedzę, dlatego skorzystaliśmy tu z klasyfikacji, jakiej dokonał Roger Clarke¹ [CLAR 1998].

Oto główne zagrożenia wymienione przez Clarke'a:

- Zagrożenia związane z transmisją danych
 - Dane mogą nie trafić do uprawnionej osoby;
 - Dane mogą trafić do nieuprawnionej osoby lub organizacji;
 - Dostęp do danych może uzyskać nieuprawniona osoba lub organizacja;
 - W trakcie transmisji danych ich zawartość może zostać zmieniona;
 - Informacja może dotrzeć do uprawnionej osoby, lecz jest to informacja nieprawdziwa;
 - Nadawca może zaprzeczyć, że wysłał dane;
 - Odbiorca może zaprzeczyć, że odebrał dane;
- Zagrożenia związane z pozostawianiem śladów aktywności w sieci
 - Pozostawianie ewidencji dotyczącej wysyłania i otrzymywania poczty
 - Pozostawianie ewidencji dotyczącej odwiedzanych stron internetowych
 - Pozostawianie ewidencji aktywności związanej z używaniem takich serwisów jak FTP, Telnet, IRC, MUD, video-phones, video-conferences
- Zagrożenia związane z tworzeniem profilu osobowego użytkownika
 - Są one w dużej mierze konsekwencją zagrożeń związanych z pozostawianiem śladów w sieci oraz analizą naszych działań pozwalającą na zebranie informacji o naszych preferencjach i zainteresowaniach. Całość informacji, jaka jest zbierana w trakcie naszych „podróży” po Internecie może być wykorzystana do stworzenia naszego profilu osobowego, który w dosyć precyzyjny sposób opisuje nasze zachowanie w sieci. Zakres informacji oraz wniosków, jakich może dostarczyć tego typu analiza może

¹ Roger Clarke – konsultant z zakresu zarządzania informacją w firmie Xamax Consultancy Pty Ltd., członek Australijskiej Akademii Nauk, od wielu lat zajmujący się problematyką ochrony prywatności.

być zaskakująco trafny. Doskonale zagadnienia te przedstawia w swoim opracowaniu Carol A. Lane [LANE 1998].

Za wyjątkiem zagrożeń związanych z transmisją danych, Clarke skoncentrował się głównie na tych, które niektórzy nazywają zagrożeniami związanymi z ochroną prywatności. Być może dla uzupełnienia listy Clarke'a warto by dodać zagrożenia związane ze zwykłym atakiem na zasoby informatyczne, w których przechowywane są dane osobowe oraz zagrożenia związane z nieumyślnym udostępnieniem tych danych, np.: poprzez błędne procedury zarządzania środowiskiem IT, ich brak czy też ich niewłaściwe stosowanie.

5. Kryteria oceny ochrony danych

Wracając do naszych usługodawców oferujących konta poczty elektronicznej, spróbujmy zastanowić się, co wpływa na ocenę poziomu ochrony naszych danych. Nasza propozycja oceny opiera się o trzy kategorie:

- Zagadnienia formalno – organizacyjne
- Zakres pozyskiwania i przetwarzania danych
- Techniczne sposoby zabezpieczenia danych osobowych

5.1 *Zagadnienia formalno – organizacyjne*

Pod terminem tym rozumiemy kwestię podejścia przez pozyskującego dane do zagadnień formalnych, takich jak:

- cel przetwarzania naszych danych,
- to czy będą one udostępniane na zewnątrz,
- czy pozyskujący pamięta o naszym prawie do wglądu w dane,
- czy pozyskujący pamięta o naszym prawie poprawiania danych,
- czy wreszcie, co jest bardzo ważne, czy pozyskujący pamięta o umożliwieniu nam ich usunięcia.

W przypadku usuwania danych interesujące jest to, w jaki sposób to usunięcie się odbywa. Czy możemy to zrobić bezpośrednio sami, czy czeka nas długa procedura oparta o wymianę korespondencji przesyłanej w tradycyjny sposób?

Niemniej ważne jest podejście do takich spraw jak odpowiedni regulamin korzystania z usługi, czy też polityka prywatności opisująca prawa, obowiązki oraz zasady ochrony prywatności użytkownika serwisu, która ostatnimi czasy, wzorem państw zachodnich, zaczęła się również pojawiać w Polsce.

Z pewnością cennym materiałem przy ocenie zagadnień formalno-organizacyjnych byłaby możliwość zapoznania się formalnymi ustaleniami organizacyjnymi administratora danych, takimi jak odpowiednie polityki i procedury. Dostęp do takich danych jest w praktyce niemożliwy i w tej materii można się tylko oprzeć na deklaracjach zachowania należytej dbałości w sprawach związanych z ochroną naszych danych, pod którymi to deklaracjami być może kryją się stosowne procedury i zapisy formalne.

5.2 Zakres pozyskiwania i przetwarzania danych osobowych

Wydaje się, że prowadzenie konta pocztowego nie powinno być związane z pozyskiwaniem od nas wielu danych osobowych. Jednak, jak łatwo zresztą się domyślić, praktyka wskazuje na coś zupełnie innego. Przy zakładaniu konta oczekuje się od nas, że podamy całą masę najróżniejszych danych. Podanie wielu z nich jest obligatoryjne i dodatkowo obarczone naszą deklaracją, co do ich poprawności. Ewidencja tego, czego się od nas oczekuje w zamian za tę usługę, naszym zdaniem wpływa na ocenę bezpieczeństwa naszych danych osobowych.

5.3 Techniczne sposoby zabezpieczania danych osobowych

Po uzyskaniu danych o użytkowniku, są one przetwarzane w systemie usługodawcy. Naturalnie powstaje więc pytanie, w jaki sposób dane te są chronione. Oczywiście odpowiedź na to pytanie nie jest łatwa. Niniejsza propozycja kryteriów oceny nie przewiduje żadnego rodzaju testów zabezpieczeń tych serwerów, na których przetrzymywane są dane. Nie oceniamy ani konfiguracji tych serwerów ani też architektury sieciowej, w której dane są przetwarzane. Pozyskanie wszystkich danych tego rodzaju wiązałoby się z przeprowadzeniem profesjonalnych testów bezpieczeństwa. Wykonywanie tego typu badań bez uzgodnień z właścicielem systemu nie jest właściwie możliwe, a przede wszystkim jest po prostu niedopuszczalne. Dlatego uwzględniliśmy aspekty o wiele bardziej proste, które zapewne w znacznej mierze

pokazują podejście usługodawcy do spraw związanych z odpowiednim zabezpieczeniem systemu, a tym pozwalają na przedstawienie ogólnej oceny poziomu bezpieczeństwa systemów usługodawcy.

W uzyskaniu takiej oceny pomagają odpowiedzi na takie pytania jak:

- Jaki jest wymagany poziom skomplikowania hasła dostępu do skrzynki pocztowej (a więc i dostępnych tam danych osobowych), (wymóg stosowania kombinacji liter i znaków alfanumerycznych)?
- Czy bierze się pod uwagę aspekty związane z zarządzaniem hasłem (np.: możliwość jego zmiany)?
- Czy zapewniona jest poufność i integralność danych wymienianych pomiędzy naszym komputerem i serwerem udostępniającym usługę? (użycie protokołu https, wykorzystującego protokół SSL (*ang. Secure Socket Layer*))

6. Badanie CERT POLSKA

CERT POLSKA w oparciu o przedstawione powyżej kryteria oceny przeprowadził badanie serwisów dostarczycieli kont pocztowych (nazywanych dalej: DKP). Poniżej znajduje się opis metodologii i wyniki tego badania.

Metodologia jak i zakres badania zostały skonsultowane z Biurem Generalnego Inspektora Ochrony Danych Osobowych.

7. Metodologia badania

Poniższe wyniki zostały uzyskane na podstawie empirycznego badania 10 największych² portali internetowych, które udostępniają zasoby swoich serwerów dla użytkowników sieci Internet, chcących uzyskać dostęp do usługi poczty elektronicznej (własne konto).

Badanie zostało przeprowadzone w miesiącu maju bieżącego roku, a uzyskane wyniki badania były weryfikowane poprzez ponowne sprawdzenie uzyskanych danych.

² Zgodnie z ustaleniami CERT POLSKA. W trakcie badania nie miały miejsca sytuacje, które zaburzałyby proces subiektywnego wyboru badanych usługodawców (np.: problemy techniczne w dostępie do serwera usługodawcy).

Wszystkie wyniki uzyskiwane były w oparciu o przeprowadzenie typowego procesu rejestracji użytkownika ubiegającego się o uzyskanie prawa do posiadania własnego konta poczty elektronicznej. Proces rejestracji przebiegał zgodnie z wytycznymi właściciela serwisu przy zachowaniu zaproponowanych przez niego procedur. Wszelkie wytyczne w postaci dodatkowych informacji i regulaminów były analizowane na bieżąco a wynikające z nich ustalenia wpływające na wyniki badań zostały uwzględnione w formularzu wynikowym.

Całość procesu stanowiącego podstawę badania nie była przeprowadzana w porozumieniu ani w ustaleniach z właścicielem DKP. W trakcie tego procesu w żaden sposób nie były naruszane zapisy regulaminu przedstawianego przez DKP jak również nie były podejmowane żadne działania, które mogłyby wpłynąć na obniżenie poziomu bezpieczeństwa lub funkcjonalności serwisu.

Zastosowane kryteria stanowią autorski zestaw CERT POLSKA i nie są kopią żadnej znanej autorom metodologii z tego zakresu. Dobór nastąpił w oparciu o przepisy ustawy o ochronie danych osobowych, posiadaną wiedzę dotyczącą praktycznych aspektów ochrony danych osobowych występujących w sieci Internet oraz zagadnień związanych z bezpieczeństwem teleinformatycznym.

Dla zastosowanych kryteriów nie zastosowano żadnych współczynników waloryzacji. Co oznacza, że w ostatecznej ocenie każde z kryteriów jest traktowane równorzędnie. Podejście takie jest podyktowane faktem, że badanie nie ma na celu stworzenie rankingu DKP a jedynie przedstawienie ogólnego stanu bezpieczeństwa danych osobowych przetwarzanych przez DKP.

8. Wyniki badania

8.1 Kryteria formalno – organizacyjne

8.1.1 Regulamin

Czy DKP posiada regulamin, w którym informuje się o tym, że przetwarzane będą dane osobowe? Czy zamieszcza podstawowe informacje dotyczące tego faktu, np.: w jakim celu dane będą przetwarzane i czy będą przekazywane podmiotom trzecim?

Okazało się, że ten postawiony przez nas wymóg jest w najlepszym stopniu spełniony przez DKP. Wszyscy (10) DKP posiadali odpowiedni, zgodny z powyższymi założeniami, regulamin.

8.1.2 Ochrona prywatności

Od pewnego czasu, w szczególności dotyczy to Stanów Zjednoczonych i Europy Zachodniej, administratorzy danych osobowych, którzy pozyskują i przetwarzają dane w Internecie posługują się czymś, co określane jest jako ochrona prywatności (*ang. Privacy policy*). Jest to dokument, w którym podmiot pozyskujący i w przyszłości przetwarzający dane osobowe, w sposób możliwie jasny i przystępny dla właściciela danych osobowych, informuje go, jakie dane będzie na jego temat zbierał, w jaki sposób będzie je przetwarzał, jakie będzie stosował środki ochrony tych danych. Polityka prywatności powinna również zawierać informacje na temat pozyskiwania danych w sposób, który może być niewidoczny dla użytkownika sieci, np.: poprzez instalację tzw. *cookies*³.

Zamieszczanie polityki prywatności nie jest równoważne podaniu podstawowych informacji dotyczących ochrony danych osobowych, które są zazwyczaj umieszczane w regulaminie. Polityka prywatności jest dokumentem fakultatywnym i może być traktowana jako wyraz szczególnej troski administratora o powierzone mu dane a tym samym jej istnienie należy potraktować jako plus dla dostarczycieli usługi.

Jak wspomniane zostało na początku tego rozdziału polityka prywatności jest już dosyć powszechnym dokumentem w innych krajach. Okazało się, że i w naszym kraju nie wygląda to tak źle. Siedmiu na dziesięciu DKP posiada i udostępnia klientom do zapoznania się tego typu dokument.

8.1.3 Prawo do poprawiania

Prawo do wglądu i poprawiania swoich danych osobowych, jak i obowiązku poinformowania właściciela danych o tym fakcie, ujęte jest w samej *ustawie o ochronie danych osobowych*, a konkretnie mówi o tym artykuł 24 tejże ustawy [UODO 1997]. Ten warunek oczywiście wszyscy DKP spełnili. Zazwyczaj już na poziomie regulaminu. Nam jednak w naszym badaniu chodziło o coś więcej. Ciekawi byliśmy czy administratorzy zadbali o to żeby tego typu czynność była możliwa do przeprowadzenia w sposób interaktywny poprzez odpowiedni interfejs na stronie internetowej

³ Opracowany przez firmę Netscape Communications mechanizm przechowywania stanu klienta przy kolejnych zadaniach kierowanych do serwera. Technika cookie pozwala zapamiętywać informacje o użytkownikach korzystających z usług internetowych. W ten sposób uzupełnia protokół HTTP, w którym nie przewidziano takiej możliwości. [NETO 2001]

administratora danych osobowych, w ramach tego samego serwisu internetowego, który posłużył do pozyskania przez administratora danych osobowych klienta. Przy rozbudowanych serwisach i dużej ilości najróżniejszych funkcjonalności, jakie oferują serwisy DKP, nie wydaje się aby był to wymóg kłopotliwy do spełnienia. Jednak wynik naszego tego nie potwierdza. Na dziesięciu DKP tylko sześciu zapewniło wspomnianą funkcjonalność.

8.1.4 Usunięcie danych osobowych

Ustaliliśmy już wcześniej, że konto u DKP jest tylko iluzorycznie kontem darmowym. Użytkownik świadomie przekazuje swoje dane osobowe, wiedząc że w zamian za to uzyska konto poczty elektronicznej. Należałoby przewidzieć, że użytkownik w pewnym momencie zrezygnuje z tej wymiany. Nie będzie zainteresowany już posiadaniem konta u DKP, ale również niechętnie będzie spoglądał na fakt posiadania przez tego DKP jego danych osobowych, dlatego chciałby usunąć własne dane osobowe z bazy danych osobowych DKP. Czy ma taką możliwość? Zadając takie pytanie również, podobnie jak w przypadku „prawa do poprawiania”, mieliśmy na uwadze to czy istnieje możliwość realizacji tego prawa w sposób interaktywny, krótko mówiąc czy mogę usunąć swoje konto pocztowe wraz z własnymi danymi osobowymi równie łatwo jak mogłem je założyć? Niestety wynik badania dotyczący tego kryterium jest bardzo niepokojący. Żaden z badanych DKP nie przedstawia takiej funkcjonalności.

8.1.5 Brak zobowiązania poprawności danych osobowych

Kryterium to potraktowaliśmy głównie jako wskaźnik informacyjny, który w naszej opinii w niewielkim stopniu wpływa na ogólną ocenę w naszym badaniu. Niemniej jednak warto wiedzieć, ilu z badanych DKP wymusza na nas zobowiązanie do tego, że podawane przez nas dane są prawdziwe. Jak łatwo się domyślić, oprócz podłoża prawnego, nie ma to specjalnego znaczenia i zapewne może posłużyć poszczególnym DKP jedynie do zapewnienia sobie możliwości pozbawiania usługi tych klientów, których dane nie zostały potwierdzone, np.: poprzez zwroty korespondencji poczty elektronicznej (przy podawaniu dodatkowego adresu poczty elektronicznej) czy też poczty tradycyjnej (przy podawaniu adresu zamieszkania lub adresu korespondencyjnego).

8.2 Cel przetwarzania danych osobowych

Podobnie jak kategoria *Brak zobowiązania poprawności danych osobowych* tak i ta kategoria ma charakter informacyjno – poglądowy i nie stanowi istotnego czynnika w ocenie poziomu ochrony danych osobowych.

Najczęściej podawanym celem przetwarzania danych osobowych, jak zresztą można było przypuszczać, był cel marketingowy (7) i cel statystyczny (5). Niepokojący jest fakt, że dwóch DKP nie podało żadnego celu, dla którego pozyskuje dane osobowe swoich klientów.

8.3 Zakres zbierania danych

Przygotowując założenia do przeprowadzenia badania uznaliśmy, że ciekawa będzie kontrola tego jak duży zakres danych ulega przetwarzaniu, czyli mówiąc w uproszczeniu ile „kosztują” darmowe konta poczty elektronicznej. Wydawałoby się, że udostępnienie tego typu usługi nie powinno się wiązać z koniecznością posiadania zbyt wielu danych na temat osób z niej korzystających. Oczywiście wskazany cel marketingowy i statystyczny przetwarzania danych jest jasny i należy się zgodzić z tym, że podajemy pewien zestaw danych osobowych, które pozwalają na stworzenie (w pewnym zakresie) naszego profilu osobowego. Trzeba przyznać, że wielu DKP tak to właśnie potraktowało i zakres danych, jaki oczekują od klienta nie jest nadmiernie wygórowany. Jednak mniej więcej połowa DKP dosyć wysoko ceni sobie własny serwis i oczekuje niemałego zestawu danych o przyszłym korzystającym z serwisu (patrz ^{Tabela}). Jak łatwo się domyślić jest to grupa, która zainteresowana jest również „zobowiązaniem do poprawności podawanych danych”. W tym wypadku danymi osobowymi, które są oczekiwane są takie dane jak: wiek, płeć, wykształcenie, sytuacja zawodowa, branża zatrudnienia czy zainteresowania. Trzeba przyznać, że wraz z danymi dotyczącymi imienia i nazwiska (3) oraz dokładnym adresem zamieszkania (2), taki zestaw danych stanowi całkiem pokaźny zasób informacji, który z pewnością posiada swoją wymierną cenę rynkową.

W przypadku tej kategorii warto również zwrócić uwagę na jeszcze jeden element stanowiący źródło informacji o korzystającym z serwisu oferowanego przez DKP. Tym elementem są wspomniane już *cookies*. Instalowanie i odczytywanie z

komputera informacji dotyczących odwiedzanych witryn internetowych może się okazać faktycznie najlepszym źródłem informacji o konkretnej osobie. Dlatego szczególnie ważny jest odnotowany przez nas fakt, że aż ośmiu na dziesięciu DKP stosowało tę właśnie technikę. Niewątpliwie zebrane w ten sposób informacje są o wiele bardziej wiarygodne i szersze niż te, które są wymagane od użytkownika w przypadku konieczności wypełnienia ankiety dotyczącej zainteresowań. Oczywiście trzeba pamiętać, że stosowanie techniki *cookie* pozwala również na profilowanie serwisu dla konkretnego użytkownika tak, aby był on dla niego wygodniejszy. W trakcie przeprowadzanego badania nie było również możliwości dokonania rozeznania czy poszczególni DKP oprócz umieszczania własnego pliku *cookie* pozyskują także dane oparte o inne pliki *cookie*, które są już zainstalowane na komputerze klienta.

8.4 Kryterium techniczne

Kryteria techniczne, jakie zastosowaliśmy, w stosunkowo wymierny sposób pozwalają na ocenę technicznego poziomu ochrony danych osobowych. W naszym badaniu ustaliliśmy sześć różnych kryteriów oceny. Zasadniczo przedstawiają one poziom ochrony poprzez stosowanie systemu haseł oraz poprzez stosowanie techniki szyfrowania transmisji.

W trakcie badania polityki zarządzania hasłami użytkowników braliśmy pod uwagę zarówno wyniki naszych działań empirycznych (np.: próba zastosowania takiego samego zestawu znaków dla loginu użytkownika oraz dla jego hasła) jak i informacje przedstawiane przez DKP, które dotyczyły haseł (np.: konieczność zastosowania minimalnej długości hasła).

8.4.1 Zróżnicowanie loginu i hasła użytkownika serwisu

Pierwszy wskaźnik, który uzyskaliśmy w czasie badania dotyczył tego czy zastosowane hasło może być dokładnie takie same, jaki jest używany login. Wynik był zaskakujący, niestety *in minus*. Tylko czterech z dziesięciu DKP wymuszało na swoich klientach, aby obydwie te wartości były różne. Zagrożenie związane z takim wynikiem jest oczywiste. Z racji tego, że dane o stosowanych nazwach użytkowników są w mniejszym lub większym stopniu dostępne, istnieje realne zagrożenie pozyskania nieautoryzowanego dostępu do wielu kont poczty elektronicznej, co wiąże się nie tylko

z dostępem do klasycznych danych osobowych, ale i z dostępem do prywatnej korespondencji klientów, poprzez zastosowanie techniki ataku na pojedyncze konto lub techniki ataku automatycznego na wiele kont.

8.4.2 Minimalna długość hasła

Tak jak wspominaliśmy we wstępie dotyczącym kryteriów technicznych ta wartość była bada poprzez deklarację, lub jej brak, DKP. Dlatego wyniki są na tyle wiarygodne na ile wiarygodna jest informacja przedstawiona przez DKP. Jakie są wyniki? Sześciu DKP określa minimalną liczbę znaków dla ustalenia hasła. Trzeba przyznać, że założenia pozytywnej oceny były dosyć liberalne i wskazanie chociażby na trzy znaki jako minimalną długość hasła było „zaliczeniem” spełnienia wymogu.

8.4.3 Znaki specjalne w haśle

Wiadomo, że w polityce zarządzania hasłami niebagatelną rolę odgrywają wymogi związane z narzuceniem konieczności stosowania przez użytkownika znaków specjalnych w haśle. Dlatego przy ocenie technicznych aspektów ochrony danych osobowych przetwarzanych przez DKP również wzięliśmy ten czynnik pod uwagę. Tym razem byliśmy bardziej rygorystyczni niż w przypadku „minimalnej długości hasła” i nie braliśmy pod uwagę instrukcji dotyczącej haseł, z jaką zapoznawał użytkownika DKP, ale z rzeczywistym stanem rzeczy, co swoją drogą okazało się podejściem słusznym, gdyż obydwie te elementy czasami różniły się od siebie, tzn. wskazanie w instrukcji na konieczność stosowania hasła nie szło w parze z wymuszeniem takiej rekomendacji w sposób techniczny. Wynik niestety nie jest korzystny. Tylko jeden z DKP zastosował w swoim serwisie technikę, która wymuszała na użytkownika zastosowanie w haśle przynajmniej jednego znaku specjalnego. Trzeba przyznać, że w tym przypadku również nie zawiesiliśmy poprzeczki zbyt wysoko, ponieważ na potrzeby naszego badania za znaki specjalne uznaliśmy nie tylko znaki typu !@#%&*^&*....., ale również cyfry.

8.4.4 **Możliwość zmiany hasła**

W tym przypadku było znacznie lepiej, najlepiej jeśli chodzi o wszystkie kryteria wśród zastosowanych kryteriów technicznych. Podkreślamy to, ponieważ możliwość zmiany hasła do usługi⁴ w naszej ocenie jest bardzo ważnym kryterium.

Siedmiu z dziesięciu DKP oferowało tę funkcjonalność w swoim serwisie.

Dobra ocena w tym przypadku nie powinna jednak sprawiać, że brak tej funkcjonalności w przypadku trzech pozostałych DKP jest naganny.

8.4.5 **Szyfrowanie**

Szyfrowanie transmisji jest narzędziem pozwalającym na zachowanie anonimowości i poufności danych. Pojęcia te niewątpliwie na stałe związane są z pojęciem korespondencji, również korespondencji elektronicznej. Niestety w trakcie naszego badania szyfrowanie nie okazało się najmocniejszą stroną badanych serwisów. Na dziesięć przypadków tylko w dwóch mieliśmy do czynienia z wymuszeniem szyfrowania sesji. Było to szyfrowanie dotyczące sesji uwierzytelnienia użytkownika, co jest oczywiście bardzo ważne. Bardzo ważna jest również, wspomniana już, kwestia zachowania poufności samej korespondencji. Niestety żaden z DKP nie pomyślał o tym, aby również odczytywanie poczty elektronicznej, poprzez korzystanie z interfejsu graficznego oferowanego przez operatora, odbywało się również w sposób bezpieczny. Choć trzeba tu w pewien sposób usprawiedliwić poddanych ocenie poprzez fakt, że tego typu funkcjonalność nie jest nadal standardem w innych zagranicznych, zazwyczaj znacznie większych, serwisach.

9. Zbiorcze zestawienie wyników badań

^{Tabela}. Poniższa tabela zawiera zbiorcze wyniki badań, zgodnie z przedstawionymi powyżej kryteriami. Na ciemniejszym tle przedstawione zostały te kryteria, które zdaniem CERT POLSKA w sposób znaczący wpływają na ocenę.

⁴ W badaniu nie było brane pod uwagę wymuszenie tej funkcjonalności a jedynie możliwość zmiany

Kryterium	Liczba DKP spełniających kryterium
Formalno – organizacyjne	
<i>Regulamin</i>	10
<i>Polityka ochrony prywatności</i>	7
<i>Prawo do poprawiania</i>	6
<i>Prawo do usuwania</i>	0
Brak zobowiązania poprawności danych osobowych	7
Cele przetwarzania danych	
Marketingowy	7
Statystyczny	5
Techniczny	1
Żaden	2
Zakres przetwarzania	
<i>Imię i Nazwisko</i>	3
<i>Adres</i>	2
<i>Zamieszkanie (przybliżone dane dotyczące miejsca zamieszkania)</i>	4
<i>Wiek</i>	5
<i>Płeć</i>	5
<i>Wykształcenie</i>	5
<i>Sytuacja zawodowa</i>	5
<i>Branża</i>	5
<i>Zainteresowania</i>	4
<i>Cookie</i>	8
Techniczno – organizacyjne	
<i>Hasło różne niż login</i>	4
<i>Minimalna długość hasła</i>	6
<i>Wymuszenie znaków specjalnych</i>	1
<i>Możliwość zmiany hasła</i>	7
<i>Szyfrowanie sesji uwierzytelnienia</i>	2
<i>Szyfrowanie sesji dostępu do poczty elektronicznej</i>	0

10. Wnioski

W naszym badaniu staraliśmy się przyjąć podstawowy zestaw kryteriów, które w naszej ocenie w poważnym stopniu mogą posłużyć do generalnej oceny stanu poziomu ochrony danych osobowych osób korzystających z darmowych serwisów poczty elektronicznej. Patrząc chociażby na opublikowaną powyżej tabelę wydaje się, że ocena ta nie jest najwyższa. Zastosowanie zwykłej średniej arytmetycznej opartej na kryteriach uznanych za najbardziej wpływających na ocenę daje wynik 4 w skali od, 1 do 10, czyli trochę gorzej niż średnio.

Z pewnością, pomijając brak możliwości usuwania własnych danych osobowych u wszystkich DKP, najlepiej wyglądają kwestie formalno – organizacyjne, związane

zazwyczaj z realizacją pewnych norm prawa i tzw. najlepszych praktyk (*ang. Best practices*) w danej dziedzinie. Gorzej jest już w organizacji zabezpieczeń technicznych, a w szczególności w kwestii zachowania poufności danych osobowych przy zastosowaniu technik kryptograficznych, których implementacja przy powszechnie używanych w Internecie technologiach ochrony transmisji nie stanowi na dzień dzisiejszy problemu, o czym może świadczyć fakt powszechnego ich wykorzystania w innych usługach internetowych jak chociażby w bankowości elektronicznej. Poniesione na ten cel nakłady organizacyjno – finansowe nie są duże.

Podsumowując należy wspomnieć jeszcze o kilku faktach, których nie wypada pominąć decydując się na przedstawienie tematu ochrony danych osobowych przez DKP:

- Korzystanie z serwisu jest dobrowolne, dlatego zawsze od użytkownika sieci będzie zależało czy zdecyduje się przekazać do przetwarzania dane osobowe dotyczące własnej osoby, w zamian za oferowane usługi.
- Wiele zagrożeń, jakie zostały przedstawione we wstępnej części tego badania nie jest rozpoznawalnych dla tzw. *statystycznego użytkownika sieci Internet*, od którego nie można oczekiwać specjalistycznej wiedzy dotyczącej technik komputerowych, a tym bardziej technik i zasad związanych z bezpieczeństwem teleinformatycznym. Dlatego to na DKP spoczywa nieformalny obowiązek zapewnienia użytkownikowi najlepszych metod ochrony.
- Badane były serwisy największych zdaniem CERT POLSKA dostawców usługi bezpłatnej poczty elektronicznej, należy przypuszczać, że ocena dotycząca pozostałych (średnich i małych) tego typu usługodawców nie jest raczej lepsza.

11. Propozycja zakresu wymagań

Niech podsumowaniem niniejszego raportu będzie próba przedstawienia zestawu wymagań podstawowych, które zdaniem CERT POLSKA mogłyby stanowić pewien wzorzec w organizacji elementów bezpieczeństwa dla serwisów oferowanych przez DKP. Mamy nadzieję, że poniższy zestaw posłuży zarówno obecnym jak i przyszłym DKP w projektowaniu systemu bezpieczeństwa danych osobowych w udostępnianych przez nich serwisach. Wierzimy również, że może on być także

pomocny *statystycznemu użytkownikowi sieci Internet*, które poważnie traktuje swoją własność, jaką niewątpliwie stanowią jego dane osobowe.

11.1 Kryteria formalno – organizacyjne

Regulamin – zasady, jakie powinny dotyczyć regulaminu zostały określone przy omawianiu tego wymogu. Regulamin powinien zawierać podstawowe informacje o przetwarzaniu danych osobowych przez administratora oraz realizować wymogi formalno – prawne, związane z przetwarzaniem danych osobowych.

Polityka ochrony prywatności – powinna zawierać informacje, w jaki sposób administrator przetwarza dane osobowe. Ważne jest również, aby w dokumencie tym znalazły się opis tego, w jaki sposób administrator chroni dane osobowe oraz jakie dane osobowe są w rzeczywistości zbierane (chodzi to uwzględnienie informacji nie tylko o danych, które są zbierane oficjalnie, ale również tych, które są zbierane innymi sposobami, np.: z wykorzystaniem techniki *cookie*).

Realizacja prawa do poprawiania – prawo do poprawiania danych jest zagwarantowane ustawowo, chodzi o to żeby administrator pozwalał na realizację tej czynności w sposób interaktywny, za pomocą odpowiedniego interfejsu dostępnego w serwisie.

Realizacja prawa do usuwania – sytuacja podobna jak w przypadku „realizacji prawa do poprawiania”. Przy spełnieniu tego wymogu użytkownik powinien móc usunąć własne dane osobowe z bazy danych administratora w sposób automatyczny. (oczywiście wiązałoby się to z rezygnacją z usługi).

Ograniczenie zakresu przetwarzania – jest to kryterium nieprecyzyjne, jednak chodzi o to, że zakres pozyskiwania danych nie powinien być zbyt szeroki w stosunku do oferowanego serwisu. W tym wypadku nie da się ustalić szczegółowych zaleceń.

11.2 Kryteria techniczne

Zróżnicowanie loginu użytkownika i hasła – użytkownik nie powinien móc ustalić takiego samego hasła i loginu (identyfikatora) użytkownika. Wymóg ten powinien być realizowany w sposób techniczny a nie jedynie poprzez zalecenie.

Określenia minimalnej długości hasła – również realizacja tego wymogu powinna się odbywać poprzez wymuszenie techniczne. Rozsądną wydaje się być propozycja stosowania minimum 6 znaków w hasle.

Stosowanie znaków specjalnych – tak jak to określiliśmy w opisie wyników badania, wymóg ten mógłby być realizowany również przy uznaniu za znak specjalny cyfr. Również nie powinna to być rekomendacja a techniczna opcja zmuszająca użytkownika do użycia choćby jednego znaku specjalnego. Należy pamiętać, aby nie doprowadzić do tego, żeby hasło składało się z samych znaków specjalnych (w tym wypadku np.: cyfr), czyli powinno ono zawierać również chociażby jedną literę.

Możliwość zmiany hasła – wymóg ten nie wymaga większych wyjaśnień – użytkownik poprzez odpowiednią funkcjonalność serwisu powinien móc zmienić swoje hasło. Przydatna byłaby również rekomendacja dotycząca częstotliwości przeprowadzania takiej zmiany (np.: co 60 dni)

Stosowanie szyfrowania sesji – wymóg ten w opcji minimum powinien być realizowany poprzez szyfrowanie tej części sesji, w trakcie której odbywa się uwierzytelnienie użytkownika. Pełna realizacja wymogu polegałaby na szyfrowaniu całości sesji, w trakcie której dochodzi zarówno do uwierzytelnienia jak i do odczytu korespondencji.

Stosowanie techniki cookie jako opcji – technika *cookie* z pewnością niesie ze sobą wiele możliwości optymalizacji serwisu, również optymalizacji z punktu widzenia użytkownika, dlatego jej stosowanie jest jak najbardziej dopuszczalne. Niemniej jednak należałoby przedstawić w sposób przystępny i obiektywny wady i zalety takiego rozwiązania (dobrym do tego miejscem jest dokument *Polityka ochrony prywatności*) oraz dać użytkownikowi opcję, dzięki której będzie mógł wybrać bardziej zoptymalizowany serwis, co się wiąże z instalacją *cookie* lub serwis podstawowy, mniej wygodny, ale bez stosowania wspomnianej techniki.

12. Literatura

[CLAR 1998] Roger Clarke – Information Privacy On the Internet Cyberspace Invades Personal Space (1998)

<http://www.anu.edu.au/people/Roger.Clarke/DV/IPrivacy.html>

[LANE 1998] Carol A.Lane – Naked In Cyberspace (1998)

<http://www.technosearch.com/naked/directory.htm>

[NETO 2001] Netopedia – <http://netopedia.techtech.pl/netopedia/>

[UODO 1997] *Ustawa o ochronie danych osobowych* (Dz.U.97.133.883 z dnia 29 października 1997 r.) <http://www.giodo.gov.pl/bgiw1220.htm>