GIODO

Generalny Inspektor
Ochrony Danych Osobowych

ABC ZAGROŻEŃ BEZPIECZEŃSTWA DANYCH OSOBOWYCH W SYSTEMACH TELEINFORMATYCZNYCH

GIODO

Generalny Inspektor
Ochrony Danych Osobowych

ABC

ZAGROŻEŃ BEZPIECZEŃSTWA DANYCH OSOBOWYCH W SYSTEMACH TELEINFORMATYCZNYCH

GIODO

Generalny Inspektor
Ochrony Danych Osobowych

Biuro Generalnego Inspektora
Ochrony Danych Osobowych

ul. Stawki 2, 00-193 Warszawa
tel. (0 22) 860 70 81
fax: (0 22) 860 70 86
kancelaria@giodo.gov.pl
www.giodo.gov.pl

Opracował
Andrzej Kaczmarek
Dyrektor Departamentu Informatyki
w Biurze GIODO

Warszawa 2009

GIODO
Generalny Inspektor
Ochrony Danych Osobowych

ABC

SPIS TREŚCI

1. Rodzaje zagrożeń, na jakie narażone są dane przetwarzane w systemach teleinformatycznych

Systemy teleinformatyczne obecnie wspomagają działania niemal we wszystkich dziedzinach życia. Są wykorzystywane w każdej nowoczesnej instytucji, zarówno dużym przedsiębiorstwie, jak i w małej firmie, urzędzie, szkole czy szpitalu. Decydują obecnie o poziomie rozwoju gospodarki państwa, jakości działania jego struktury organizacyjno-administracyjnej, szeroko rozumianym bezpieczeństwie, jak również poziomie życia obywateli.

Rozwój sieci telekomunikacyjnych i usług sieciowych, który nastąpił w ostatnich latach, spowodował, że zarówno duże organizacje, jak i małe podmioty, w tym osoby fizyczne, w coraz większym stopniu są uzależnione od sprawności i bezpieczeństwa użytkowanych systemów teleinformatycznych. Są one pomocne do wyszukiwania różnorodnych informacji, robienia zakupów czy przekazywania bankowi dyspozycji w zakresie wykonania określonych operacji.

Jak wynika z wielu badań, z usług oferowanych przez systemy teleinformatyczne korzystałoby jeszcze więcej osób, gdyby nie obawa przed cyberprzestępczością, której celem jest pozyskanie poufnych informacji, kradzież środków pieniężnych z banków, dorobku intelektualnego lub rozprowadzanie prawnie zakazanych informacji i materiałów.

Obawy te są w pełni uzasadnione. Nasilenie działań przestępczych skierowanych na kradzież i nielegalne wykorzystanie informacji w sieciach telekomunikacyjnych systematycznie wzrasta, tak jak wzrasta liczba dostępnych usług i wielkość zgromadzonych w sieci zasobów informacyjnych. Najpoważniejsze z zagrożeń to ataki hakerów – programistów posiadających szeroką wiedzę informatyczną, którzy wykorzystują luki w oprogramowaniu i bezpieczeństwie systemów informatycznych, oraz ataki przestępców komputerowych, zwanych również crakerami, którzy do celów przestępczych wykorzystują wiedzę i/lub procedury opublikowane przez hakerów oraz nieświadomość i naiwność użytkowników.

Ci pierwsi to programiści o bardzo dużych, praktycznych umiejętnościach informatycznych, wyszukujący luki w bezpieczeństwie systemów i tworzący kody programów, które pozwalają obejść stosowa-

ne zabezpieczenia. Metody ich działania zmieniają się stosownie do przeobrażeń, jakie występują w technikach programowania i wykorzystywania nowych technologii. Generalnie hakerzy koncentrują się na łamaniu zabezpieczeń systemów teleinformatycznych po to, aby wykazać możliwość zmieniania treści przetwarzanych danych oraz uzyskiwania do nich dostępu. Ich działania mają na celu przede wszystkim informowanie administratorów i producentów oprogramowania o wykrytych lukach, a często również informowanie opinii publicznej o dokonaniu ataku dla podkreślenia własnych umiejętności i zdobycia w ten sposób uznania w środowisku. Działania hakerów rzadko mają na celu wyrządzenie szkody instytucjom lub osobom, których dane są przetwarzane, ale wyniki ich pracy mogą być wykorzystane przez inne osoby – crakerów w celach typowo przestępczych.

Crakerzy z kolei to osoby, które stosując dostępne w sieci narzędzia programowe, wykorzystują je w celach przestępczych, np. do przechwycenia uprawnień dostępu do cudzego konta w systemie informatycznym banku, operatora telefonicznego itp. w celu wykonania na swoją korzyść określonych działań lub pozyskania cennych informacji, np. projektów chronionych prawem autorskim, tajemnicą przedsiębiorstwa bądź innych danych chronionych, jak np. dane osobowe. W zależności od celu i skuteczności ataku, wyrządzone szkody mogą mieć charakter czysto ekonomiczny (np. kradzież środków finansowych), szpiegowski (np. kradzież informacji, m.in. handlowej, naukowo-technicznej, technologicznej, organizacyjnej itp.), a także społeczny (utrata zaufania, reputacji). W literaturze nie zawsze rozróżnia się wymienione typy działań i obydwie grupy osób zalicza się do tzw. cyberprzestępców.

Odrębna kategoria zagrożeń związanych z wykorzystywaniem nowych technologii informacyjnych wynika z nieświadomości użytkowników co do istniejących zagrożeń i nieprzestrzegania przez nich zaleceń dotyczących bezpiecznego korzystania z systemów informatycznych. Skutkuje to podatnością na wykonywanie zagrażających bezpieczeństwu operacji, do czego użytkownik może być nakłaniany poprzez pocztę elektroniczną, zamieszczenie linków na stronach internetowych lub inne formy komunikacji, takie jak komunikatory internetowe, portale społecznościowe itp.

Rozważając zagrożenia dla bezpieczeństwa informacji, szczególną uwagę należy zwrócić na zagrożenia zewnętrzne wynikające z połączeń telekomunikacyjnych systemu informatycznego użytkownika czy administratora z innymi systemami i sieciami zewnętrznymi. Zagrożenia te można podzielić na trzy następujące grupy: podsłuch, manipulacja, podstawienie oraz ich kombinacje – np. podsłuch-podstawienie i inne.

1.1. Podsłuch

Podsłuch charakteryzuje się tym, że mimo dostarczenia do odbiorcy informacji o niezmienionej treści, ich poufność zostaje naruszona. Typowym przykładem podsłuchu jest równoległe podłączenie się intruza do kanału komunikacyjnego i „podsłuchiwanie" przesyłanych informacji. W przypadku linii telefonicznej może to być podsłuch prowadzonej rozmowy lub jej nieuprawnione nagrywanie w celu późniejszego wykorzystania. W przypadku transmisji danych będzie to zapisywanie przekazywanych informacji na zainstalowanym nośniku w miejscu „podsłuchu" lub równoległe jej kierowanie do adresata i do systemu informatycznego intruza w celu dalszego przetwarzania i wykorzystywania przez podsłuchującego lub jej odsprzedaży innym, zainteresowanym podmiotom.

1.2. Manipulacja

Manipulacja polega na uzyskaniu dostępu do danych i ingerowaniu w ich treść. Może być ona wykonywana na danych, które w danej chwili są zlokalizowane na komputerach uczestniczących w przetwarzaniu danych lub na danych, które w danej chwili znajdują się w medium transmisyjnym sieci telekomunikacyjnej.

1.3. Podstawienie

Podstawienie polega na dostarczeniu odbiorcy/systemowi określonej informacji lub wykonaniu działań przez stronę, która podaje fałszywą tożsamość w celu uzyskania odpowiednich uprawnień. Przykładem podstawienia może być wysłanie wiadomości elektronicznej ze sfałszo-

wanym adresem nadawcy albo wykonanie określonych operacji w systemie po uzyskaniu dostępu do określonych zasobów w wyniku użycia uprawnień innej osoby. W tym ostatnim przypadku mamy do czynienia z tzw. kradzieżą tożsamości, zjawiskiem, które od kilku już lat powoduje ogromne straty. Tylko w Stanach Zjednoczonych, według badań firmy Javelin Strategy & Research, straty spowodowane infekcją szkodliwego oprogramowania i kradzieżą tożsamości w 2008 r. szacuje się na 1,5 mld dolarów[1]. Dla przestępców wykorzystujących cudzą tożsamość najważniejsze jest zdobycie – różnymi dostępnymi metodami – takich danych należących do użytkowników, które służą im do uzyskania dostępu do danego systemu, jak: identyfikator, hasło, pin, karta dostępowa itp. Dane te przestępcy uzyskują, wykorzystując najczęściej luki w zabezpieczeniach systemów lub nieświadome, nierozważne, a często bezmyślne postępowanie samych użytkowników.

1.4. Kombinacje: podsłuch – podstawienie i inne

W praktyce wymienione wyżej formy działań przestępczych mogą być stosowane w określonych ciągach skutkowo-przyczynowych. Dotyczy to szczególnie kombinacji podsłuch – podstawienie, gdzie uzyskane w wyniku podsłuchu dane służące uwierzytelnieniu wykorzystane mogą być do uzyskania nieuprawnionego dostępu do systemu informatycznego i wykonania określonych operacji podstawienia.

Żeby skutecznie bronić się przed wymienionymi działaniami przestępczymi, należy dobrze poznać zarówno podatność na zagrożenia sieci telekomunikacyjnych i systemów informatycznych, jak i stopień wiedzy technicznej użytkowników, którzy z nich korzystają. Skuteczna ochrona przed zagrożeniami zewnętrznymi wymaga współdziałania producentów oprogramowania, dostawców usług sie-

[1] Wg raportu firmy Javelin Strategy & Research, średni koszt kradzieży tożsamości w ostatnim roku w Stanach Zjednoczonych wyniósł około 496 dolarów. Koszty zaś związane z usuwaniem skutków kradzieży tożsamości w skali ostatniego roku oszacowano na 90 mln godzin.

ciowych, a także staranności użytkowników w stosowaniu określonych zasad bezpieczeństwa.

Dla bezpieczeństwa informacji, w tym właściwego zabezpieczenia danych osobowych, szczególne znaczenia ma zapewnienie odpowiednich działań profilaktycznych i naprawczych, zarówno dotyczących rozwiązań informatycznych, jak i przestrzegania przepisów o ochronie danych osobowych.

2. Dane osobowe w systemach informatycznych

Zgodnie z art. 6 ust. 1 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. nr 101, poz. 926 z późn. zm.), zwanej dalej „ustawą", za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. W definicji tej bardzo istotne znaczenie ma to, że za dane osobowe uważa się nie tylko dane dotyczące osób już zidentyfikowanych, ale również dane dotyczące osób możliwych do zidentyfikowania. Przy czym za osobę możliwą do zidentyfikowania uważa się osobę, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne (art. 6 ust. 2 ustawy). Użyte w cytowanej definicji kryterium oceny, jakie należy stosować przy przyznawaniu informacjom statusu danych osobowych, jest nieostre, zwłaszcza w świetle art. 6 ust. 2 i 3. Użyte np. w art. 6 ust. 2 ustawy sformułowanie „pośrednio" może być różnie rozumiane, chociażby co do liczby stopni pośrednictwa. Podobnie różnie w znaczeniu ilościowym można interpretować użyte w art. 6 ust. 3 kryterium kosztów, czasu i działań. Użyta tam miara tych środków określona słowem „nadmiernych" może być różnie interpretowana w zależności od wielu czynników, np. relacji wartości określonych danych do kosztów działań, jakie należy podjąć w celu ich uzyskania czy też zamożności osoby lub podmiotu poszukującego danych informacji.

Pośrednia możliwość identyfikacji osoby, której dane dotyczą, ma zasadnicze znaczenie w odniesieniu do danych przetwarzanych

w systemach teleinformatycznych, szczególnie do tych danych, które służą rozpoznawaniu i uwierzytelnianiu się użytkowników, takich jak adres e-mail, *nick*, login czy wszelkiego rodzaju oznaczenia urządzeń końcowych w sieciach teleinformatycznych, takie jak adresy IP komputerów czy numery telefonów. Omówiona wyżej definicja danych osobowych nie precyzuje, które z wymienionych kategorii informacji mają status danych osobowych, a jedynie wskazuje, czym należy się kierować przy klasyfikowaniu informacji jako dane osobowe. Dlatego do każdego przypadku przetwarzania wymienionych wyżej kategorii danych należy podchodzić indywidualnie, badając przede wszystkim to, czy dotyczą one osób, a także wszelkie okoliczności związane z możliwością identyfikacji osób. Istotną wskazówką dla takiej analizy jest punkt 26 preambuły do dyrektywy 95/46/WE[2], który stanowi, że „w celu ustalenia, czy daną osobę można zidentyfikować, należy wziąć pod uwagę wszystkie sposoby, jakimi może posłużyć się administrator danych lub inna osoba w celu zidentyfikowania owej osoby".

Warto przy tym zwrócić uwagę na fakt, że w większości przypadków osoby lub podmioty korzystające z usług dostępu do sieci teleinformatycznych albo telekomunikacyjnych związane są z dostawcami tych usług stosownymi umowami[3], w których dokładnie określona jest ich tożsamość. Dostawcy tych usług posiadają wiele szczegółowych informacji dotyczących działalności swoich abonentów w kontekście świadczonych im usług, w tym dane lokalizacyjne i dane o ruchu telekomunikacyjnym[4].

[2] Dyrektywa 95/46/WE Dyrektywa Parlamentu Europejskiego i Rady z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych.

[3] Poza przypadkami, gdzie abonent znany jest dostawcy usług, występują przypadki anonimowych usług, jak np. usługi telefonii komórkowej w systemie przedpłat czy też dostaw usług internetowych poprzez tzw. hotspoty lub kafejki internetowe.

[4] Więcej na temat danych lokalizacyjnych oraz danych o ruchu patrz pkt. 14 i 15 preambuły do Dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z 12 lipca 2002 r. w sprawie przetwarzania danych osobowych oraz ochrony prywatności w sektorze komunikacji elektronicznej (Dyrektywa o ochronie prywatności i komunikacji elektronicznej).

Dane lokalizacyjne to dane o położeniu geograficznym abonenta w określonym czasie, takie jak długość i szerokość geograficzna oraz wysokość n.p.m., które można wzbogacić o dane z map i planów miejscowości na danym obszarze. Za ich pomocą można również określić kierunek podróży oraz szybkość przemieszczania się.

Dane dotyczące ruchu telekomunikacyjnego to m.in. dane o: wyborze drogi (*routing*), czasie rozpoczęcia i zakończenia połączenia, ilości przekazywanych informacji (w przypadku transmisji danych), wykorzystanym protokole, wyposażeniu terminala nadawcy lub odbiorcy, sieci źródłowej lub sieci końcowej.

Charakter danych osobowych mogą mieć także inne informacje, takie jak pliki *cookies*, numer MAC karty sieciowej, rejestr odwiedzanych stron czy numer IMEI telefonu komórkowego, gdyż mogą być one wykorzystane przez inne podmioty do identyfikacji osób oraz głębszego poznawania ich potrzeb, zainteresowań, preferencji itp. Informacje takie, zgodnie z art. 6 ust. 1 ustawy, należy klasyfikować jako dane osobowe, jeżeli możliwe jest ustalenie osoby, której dotyczą bez angażowania, w ten proces nadmiernych kosztów, czasu lub działań.

W celu określenia, w jakich okolicznościach wymienione wyżej informacje należy uznać za dane osobowe, a także dla zapewnienia właściwego ich przetwarzania, warto kierować się polskimi przepisami regulującymi ochronę danych osobowych oraz takimi unijnymi aktami prawnymi i opiniami Grupy Roboczej Art. 29 do spraw ochrony danych osobowych[5], jak:

- Konwencja Nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych z 28 stycznia 1981 r.,

[5] Grupa robocza została powołana na mocy art. 29 Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych. Jest ona niezależnym europejskim organem doradczym w zakresie ochrony danych i prywatności, którego zadania określają przepisy art. 30 Dyrektywy 95/46/WE i art. 15 Dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej).

- Rekomendacja R(99) 5 Rady Europy z 23 lutego 1999 r. dotycząca ochrony prywatności w Internecie oraz Aneks do Rekomendacji zawierający wskazówki dotyczące przetwarzania danych osobowych w związku ze zbieraniem i przetwarzaniem danych osobowych w sieciach teleinformatycznych,
- Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych,
- Opinia 2/2002 Grupy Roboczej Art. 29 w sprawie dotyczącej używania unikalnych identyfikatorów końcowych urządzeń telekomunikacyjnych na przykładzie IPv6 przyjęta 30 maja 2002 r.,
- Opinia 4/2004 Grupy Roboczej Art. 29 w sprawie przetwarzania danych osobowych przy nadzorze z użyciem kamer video przyjęta 11 lutego 2004 r.,
- Opinia 4/2007 Grupy Roboczej Art. 29 w sprawie pojęcia danych osobowych przyjęta 20 czerwca 2007 r.,
- Opinia 1/2008 Grupy Roboczej Art. 29 dotycząca zagadnień ochrony danych związanych z wyszukiwarkami przyjęta 4 kwietnia 2008 r.

Zarówno w Konwencji Nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, jak i w Dyrektywie 95/46/WE Parlamentu Europejskiego i Rady z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych przyjęto szeroką definicję danych osobowych. Jest ona zbieżna z definicją zawartą w polskiej ustawie o ochronie danych osobowych, co jest istotne przy korzystaniu z opinii zawartych w Rekomendacjach Rady Europy, jak i opiniach Grupy Roboczej Art. 29.

Danymi osobowymi w rozumieniu dyrektywy są wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Pojęcie danych osobowych obejmuje informacje dostępne w jakiejkolwiek formie (np. alfabetycznej, liczbowej, graficznej, dźwiękowej), zapisane na nośnikach tradycyjnych (papier, płótno, tablice itp.) lub na nośnikach elektronicznych (taśma magnetofonowa, dyski magnetyczne i inne).

We wskazówkach dotyczących przetwarzania danych osobowych w związku ze zbieraniem i przetwarzaniem danych osobowych w sieciach teleinformatycznych dołączonych do Rekomendacji R(99) 5 Rady Europy z 23 lutego 1999 r. dotyczącej ochrony prywatności w Internecie za dane osobowe uznano adresy poczty elektronicznej, które odnoszą się do osób fizycznych.

Z kolei w Opinii 4/2007 w sprawie pojęcia danych osobowych przyjętej przez Grupę Roboczą Art. 29 ds. ochrony danych osobowych 20 czerwca 2007 r. wskazano, że celem przepisów dyrektywy 95/46/WE jest ochrona osób, których dane dotyczą, dlatego z jednej strony należy unikać zawężającej interpretacji pojęcia danych osobowych i zachowywać w tym względzie odpowiednią elastyczność, z drugiej zaś, jego zakres nie powinien być nadmiernie rozszerzany.

Co ważne, opinia Grupy Roboczej Art. 29 rozpatruje pojęcie danych osobowych w kontekście czterech ściśle powiązanych ze sobą elementów:

- „wszelkie informacje" – należy przez to rozumieć informacje niezależnie od charakteru lub treści oraz formatu technicznego (nośnika, na którym są zawarte). Za dane osobowe należałoby również uznać odwzorowania danych biometrycznych oraz dane DNA, które mogą być wykorzystywane w celu ustalenia tożsamości osób,
- „dotyczy" – związek określonej informacji z określoną osobą może być ustalony na podstawie treści informacji (informacje na temat danej osoby), celu wykorzystywania informacji (np. ocena danej osoby) lub skutku, jaki wywołuje określona informacja (np. wpływ na prawa

i interesy określonej osoby). Związek danej informacji z osobą, której ona dotyczy może być ustalony również na podstawie danych o źródle ich pochodzenia lub danych uzyskanych z tego źródła,

- „zidentyfikowana lub możliwa do zidentyfikowania" osoba fizyczna – odróżnienie lub możliwość odróżnienia osoby spośród danej grupy może nastąpić na podstawie różnych informacji (tzw. czynników identyfikujących), które mogą zostać powiązane z daną osobą. Analizując ten element definicji danych osobowych, szczególną uwagę warto zwrócić na możliwość pośredniej identyfikacji osoby, tj. możliwość identyfikacji osoby na podstawie powiązania posiadanych informacji z innymi informacjami (np. zarejestrowane obrazy pochodzące z monitoringu video, numery IP komputerów podłączonych do Internetu, pseudonimy użytkowników korzystających z usług internetowych),
- „osoby fizyczne" – tylko żyjące osoby fizyczne są co do zasady objęte ochroną. Jednak w niektórych przypadkach informacje o osobach zmarłych mogą dotyczyć również osób żyjących (np. informacja o chorobach dziedzicznych) i wówczas zakres ochrony powinien zostać rozciągnięty również na tego rodzaju informacje. Ponadto ochronę informacji dotyczącej osób zmarłych mogą wprowadzać również przepisy szczególne (np. obowiązek zachowania tajemnicy medycznej, ochrona wizerunku i czci osoby zmarłej). W niektórych przypadkach dopuszczalne wydaje się również uznanie informacji o osobach prawnych za informację dotyczącą osób fizycznych (np. gdy nazwa osoby prawnej pochodzi od nazwiska osoby fizycznej; firmowa poczta pracownika używana jest przez konkretnego pracownika firmy). W tego rodzaju przypadkach analizie poddać należy treść informacji, jej cel lub skutek, jaki może wywołać.

2.1. Numer telefonu

Numer telefonu jest ciągiem cyfr identyfikujących zakończenie sieci telefonicznej przypisane abonentowi przez operatora telefonicznego. Jego wybranie za pomocą urządzeń telekomunikacyjnych (telefon,

telefaks, modem) powoduje nawiązanie (zestawienie) połączenia z żądanym abonentem. Numery te przetwarzane są przez operatorów telefonicznych (zarówno tradycyjnych, jak i komórkowych) w rejestrach umów oraz w systemach technicznych realizujących połączenia. Rejestr umów zawiera dane łączące numer telefonu z danymi abonenta (osoby prywatnej lub firmy) oraz inne warunki umowy. Rejestr techniczny zawiera z kolei dane o ruchu telefonicznym, czyli dane na temat wykonywanych połączeń telefonicznych, na które składają się m.in. wybierane przez abonenta numery, data i czas rozpoczęcia połączenia, czas jego trwania, koszt impulsu itp. Dane te przyporządkowane są do określonego zakończenia linii telefonicznej (numeru telefonu), z którego wykonywane były połączenia. W tej sytuacji, jeżeli telefon o wskazanym numerze przyporządkowany był do określonej, znanej operatorowi osoby, to powyższe dane można klasyfikować jako dane osobowe.

Rozważając każdy z tych rejestrów niezależnie, można wskazać, iż w przypadku rejestru abonentów mamy do czynienia z klasycznym zbiorem danych osobowych, gdzie zestaw danych o numerze telefonu wraz z danymi abonenta, który dysponuje danym numerem jest zbiorem danych dotyczących osób już zidentyfikowanych. Zbiór ten zawiera wprost w swej strukturze dane, które jednoznacznie identyfikują osobę, której dotyczą. W przypadku rejestru technicznego mamy do czynienia z informacjami, które nie zawierają danych wprost identyfikujących osobę, której dotyczą. Dopiero po ich odpowiednim powiązaniu z danymi z rejestru abonentów będą one odnosić się do jednoznacznie zidentyfikowanej osoby. Zgodnie z przytoczoną definicją danych osobowych, dane z rejestru technicznego są zatem danymi, które pośrednio mogą dotyczyć zidentyfikowanych osób, gdyż nie zawierają w swojej strukturze informacji, które wprost identyfikują osobę, której dotyczą. Status wymienionych wyżej rejestrów prowadzonych przez operatorów telefonicznych jest powszechnie znany i jednoznacznie rozumiany jako rejestry danych osobowych.

Dla obydwu kategorii danych przetwarzanych w wymienionych rejestrach przewidziana jest prawna ochrona ich poufności. Dane o abonentach telefonicznych chronione są głównie na podstawie usta-

wy o ochronie danych osobowych, dane z rejestru technicznego natomiast, nazywane często danymi o ruchu telekomunikacyjnym, zarówno na podstawie ustawy o ochronie danych osobowych, jak i ustawy Prawo Telekomunikacyjne[6], która dodatkowo zapewnia ochronę danych o ruchu telekomunikacyjnym[7]. Zgodnie z art. 159 ust. 2 Prawa telekomunikacyjnego, zapoznawanie się, utrwalanie, przechowywanie, przekazywanie lub inne wykorzystanie treści lub danych objętych tajemnicą telekomunikacyjną przez osoby inne niż nadawca i odbiorca komunikatu jest możliwe tylko wtedy, gdy:

- będzie to przedmiotem usługi lub będzie to niezbędne do jej wykonania,
- nastąpi to za zgodą nadawcy lub odbiorcy, których dane dotyczą,
- jest niezbędne w celu rejestracji komunikatów i związanych z nimi danych transmisyjnych dla celów zapewnienia dowodów transakcji handlowej,
- jest konieczne z innych powodów przewidzianych ustawą lub przepisami odrębnymi.

W tym ostatnim przypadku (ujawnienie danych objętych tajemnicą telekomunikacyjną z innych powodów przewidzianych ustawą lub przepisami odrębnymi) jednostkami uprawnionymi do zapoznania się z informacją przekazywaną za pośrednictwem sieci telekomunikacyjnych są sądy, prokuratura oraz jednostki organizacyjne podległe ministrowi obrony narodowej lub przez niego nadzorowane, uprawnione organy i jednostki organizacyjne nadzorowane lub podległe ministrowi właściwemu do spraw wewnętrznych, ministrowi właściwemu do spraw finansów publicznych, Szefowi Agencji Bezpieczeństwa Wewnętrznego, Szefowi Agencji Wywiadu, Szefowi Centralnego

[6] Ustawa z 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. nr 171, poz. 1800 z późn. zm.).

[7] Tajemnica telekomunikacyjna zdefiniowana w art. 159 Prawa telekomunikacyjnego obejmuje: dane dotyczące użytkownika, treści indywidualnych komunikatów, dane transmisyjne, dane lokalizacyjne oraz dane o próbach uzyskania połączenia.

Biura Antykorupcyjnego oraz służbom wywiadu i kontrwywiadu wojskowego.

2.2. Numer IP

Numer IP – nazywany również adresem IP – jest liczbą służącą do oznaczenia modułu technicznego urządzeń komputerowych (komputerów, drukarek, kamer, a nawet urządzeń AGD i RTV itp.) umożliwiającego połączenie danego urządzenia z siecią telekomunikacyjną. Moduły te nazywane powszechnie interfejsem sieciowym zapewniają właściwą komunikację tych urządzeń między sobą. Dlatego bardzo często mówi się, że numer IP służy do wskazania urządzeń w danej sieci teleinformatycznej i przypisywany jest do urządzenia, np. komputera, drukarki, kamery itp. Urządzenia te przypisane mogą być do konkretnej osoby fizycznej. Numer IP może być wykorzystywany również do oznaczenia określonej grupy urządzeń sieciowych bądź całej sieci komputerowej opartej na protokole IP. W sieci Internet numer IP komputera nadawany jest przez dostawcę Internetu w ramach posiadanej przez niego puli adresowej otrzymanej od organizacji RIPE NCC[8], która koordynuje przydział tych adresów w całej Europie, na Bliskim Wschodzie i w części Azji.

W systemach informatycznych dostawców Internetu, podobnie jak u operatorów telefonicznych, przetwarzane są przede wszystkim dwa rodzaje danych:

- dane o abonentach zawierające numer publiczny IP w powiązaniu z danymi osobowymi abonenta (osoby prywatnej) lub danymi firmy,
- dane o ruchu telekomunikacyjnym, czyli dane na temat wykonywanych połączeń teleinformatycznych składających się m.in. z nume-

[8] RIPE NCC (RIPE *Network Coordination Centre*) – organizacja zajmująca się zarządzaniem zasobami internetowymi (adresy IPv4, IPv6) w regionie Europy, Bliskiego Wschodu i części Azji: RIPE NCC (http://www.ripe.net/info/ncc/index.html). Przydziela adresy IP firmom i organizacjom ze swojego regionu. RIPE NCC zajmuje się także wsparciem technicznym dla RIPE (fr. *Réseaux IP Européens* – Europejska Sieć IP) – stowarzyszenia z siedzibą w Amsterdamie zajmującego się rozwojem Internetu.

rów IP urządzeń, między którymi nawiązywane były połączenia, daty i czasu rozpoczęcia i zakończenia tych połączeń, rodzaju tych połączeń.

Dane o abonentach internetowych, porównane wcześniej do danych o abonentach telefonicznych, są danymi osobowymi, które wprost odnoszą się do zidentyfikowanych osób. Dane o ruchu telekomunikacyjnym natomiast (tzw. logi systemowe serwerów i innych urządzeń sieciowych, które pośredniczą w realizacji połączenia), zawierające dane techniczne dotyczące połączeń, w tym numery IP komputerów, datę i czas połączenia, informacje o adresach przeglądanych stron, wykonywanych wpisach na forach dyskusyjnych itp., nie zawierają wprost danych identyfikujących osoby. Jeżeli jednak dane opisujące ten ruch dotyczą ruchu generowanego przez stację komputerową osoby fizycznej, której tożsamość można zidentyfikować poprzez zapytanie skierowane do operatora danej sieci lub na podstawie innych informacji, to należy uznać, że dane takie są również danymi osobowymi. Są to bowiem dane odnoszące się do osób, których tożsamość nie jest jeszcze ustalona, ale jej ustalenie jest możliwe.

Adresu IP komputera lub innego urządzenia sieciowego, np. drukarki, kamery, nie będzie można uznać za informację spełniającą wymogi definicji danych osobowych, jeśli urządzenie, do którego jest on przypisany, znajduje się w dyspozycji podmiotu niebędącego osobą fizyczną i nie można wskazać jednoznacznie osoby, która sprawuje nad nim wyłączną kontrolę. Tak więc danymi osobowymi nie będą np. adres IP serwerów wyszukiwarki internetowej www.google.pl czy adres serwera poczty elektronicznej firmy Onet.pl. Jest to sytuacja podobna do numeru telefonicznego, który jest przypisany do aparatu telefonicznego zainstalowanego w miejscu publicznym, np. w budce telefonicznej na ulicy, dworcu kolejowym, hali lotniska itp.

2.3. Login

Pod pojęciem „login” rozumie się ciąg znaków (słowo) służące do jednoznacznego określenia użytkownika lub procesu w systemie in-

formatycznym. Login jest stosowany do zidentyfikowania użytkownika (ang. *user identifier*) w sieci komputerowej lub komputerowym systemie wielodostępnym, a w systemie informatycznym do „powiązania" użytkownika z przydzielonymi mu uprawnieniami oraz do oznaczenia wykonywanych przez niego operacji. Stąd też login jest niezbędnym elementem procesu kontroli dostępu podczas rozpoczynania przez użytkownika pracy w systemie. W procesie tym następuje weryfikacja, czy użytkownik o wskazanym identyfikatorze jest w systemie zarejestrowany oraz czy wprowadzone przez niego hasło lub inne dane uwierzytelniające są zgodne z tymi, jakie zostały przez tego użytkownika ustalone. System zaś, wykorzystując uprawnienia, jakie danemu użytkownikowi przyznano do poszczególnych zasobów, zezwala lub zabrania mu na wykonywanie określonych operacji.

W przypadku administratora systemu informatycznego, który ściśle kontroluje nadawane innym użytkownikom uprawnienia, identyfikator użytkownika jest najczęściej powiązany z innymi danymi o osobie, której jest on przypisany, takimi jak imię, nazwisko, stanowisko, miejsce pracy, numer telefonu, przyznane uprawnienia itp. Dane te przypisywane są do danego identyfikatora w procesie tzw. rejestracji użytkownika w systemie informatycznym. Ich poprawność jest weryfikowana podczas rejestracji, co sprawia, że dane te odnoszą się do zidentyfikowanych osób fizycznych, a więc są danymi osobowymi.

Nie zawsze jednak powiązania między identyfikatorem użytkownika i innymi informacjami o osobie, której został on przypisany, są weryfikowane pod kątem ich prawdziwości, czy rzeczywiście wskazują one na osobę, która danym identyfikatorem ma się posługiwać. Weryfikacji takiej nie ma np. w portalach internetowych, gdzie osoba podczas zakładania konta użytkownika o zdefiniowanych odgórnie uprawnieniach sama wpisuje swoje dane rejestracyjne i dane te nie są sprawdzane pod względem zgodności ze stanem faktycznym.

Identyfikator użytkownika (login) w systemie informatycznym służy zatem do rozpoznania danego użytkownika, do zidentyfikowania jego uprawnień w zakresie operacji, które może wykonywać w danym systemie, oraz do oznaczenia tych operacji, które wykonał. Dlatego

identyfikator użytkownika w danym systemie (login) powinien być dla każdego użytkownika unikatowy. Nie ma przeszkód natomiast, aby w innym systemie taki sam login istniał i należał do innego użytkownika[9].

W niektórych systemach zakres danych powiązanych z nazwą użytkownika może być znacznie ograniczony. Z sytuacją taką mamy do czynienia w przypadku użytkowników forów dyskusyjnych, których nazwy nie wiąże się z danymi określającymi uprawnienia (każdy użytkownik ma takie same uprawnienia). Nazwę tę wykorzystuje się np. tylko do oznaczenia wpisów wprowadzonych na forum przez danego użytkownika. W tych ostatnich przypadkach login nazywany jest często nazwą „*nick*" (z ang. *nickname* – przezwisko, pseudonim) i tworzony jest w taki sposób, aby wprost nie stanowił danych identyfikujących daną osobę.

2.4. *Nick*

Nick to ciąg znaków (słowo) tworzący nazwę, pod jaką dana osoba chce występować, jeśli nie chce się posługiwać swoim imieniem lub/i nazwiskiem. Biorąc pod uwagę serwisy internetowe, np. portale społecznościowe, *nick* może być tożsamy z nazwą użytkownika, służącą do identyfikacji osoby (zamiennie używane są nazwy login, *user*, użytkownik, identyfikator). Pod pojęciem nick rozumie się również nazwę używaną do podpisania wiadomości umieszczanych na forach dyskusyjnych, podpisywania komentarzy zamieszczanych na portalach informacyjnych, oznaczania osób uczestniczących w czatach, osób biorących udział w dyskusjach na IRCu[10] czy też nazwę użytkownika w komunikatorach internetowych. W zależności od rodzaju usługi, nazwa *nick* może mieć charakter tymczasowy, użyty w czasie *ad-hoc* (np.

[9] Sytuacje, w których takie same nazwy login w różnych systemach mogą wskazywać na różne osoby dotyczy zazwyczaj systemów internetowych, w których wyboru nazwy użytkownika (loginu) dokonuje sam użytkownik w procesie rejestracji. W systemach takich osoba rejestrująca się może wskazać tylko taką nazwę (login), która nie została jeszcze użyta przez inne osoby.

[10] IRC (ang. *Internet Relay Chat*) – usługa umożliwiająca wymianę komunikatów tekstowych w trybie on-line pomiędzy użytkownikami Internetu (jeden z pierwszych komunikatorów internetowych).

na czacie dla oznaczenia osoby na czas jej udziału w dyskusji czy skomentowania wydarzenia w portalu informacyjnym) albo stały (w przypadku użytkowników rejestrowanych na forach dyskusyjnych, w portalach społecznościowych itp.).

Korzystając z *nicku* tymczasowego, przy każdym połączeniu się z daną usługą ta sama osoba może występować pod inną nazwą (*nickiem*).

Większość usług internetowych oferuje możliwość używania *nicków* zarówno stałych, jak i tymczasowych. Charakterystyczne dla *nicków* stałych jest to, że w danym serwisie oznaczają one zawsze tę samą osobę. W celu uniemożliwienia użycia przez inną osobę tego samego *nicku*, *nick* stały jest chroniony hasłem, które powinno być znane tylko przez tę osobę, która dany *nick* wybrała. Ta sama osoba, uczestnicząc w różnych serwisach, może występować pod różnymi stałymi nazwami (*nickami*). Może się również zdarzyć, że ta sama osoba w jednym czacie lub serwisie może wystąpić w dwóch lub więcej „wcieleniach", używając za każdym razem innego *nicku*. Bardzo często zdarza się, że w różnych serwisach internetowych ten sam *nick* tymczasowy używają różne osoby. Przykładem takiej sytuacji mogą być serwisy internetowe umożliwiające zamieszczanie wpisów z pozycji niezarejestrowanego użytkownika, czyli takiego, który nie założył sobie w danym serwisie konta użytkownika z przypisanym do niego stałym identyfikatorem. Wpisy takie oznaczane są często słowem „gość" lub częścią publicznego numeru IP komputera, z którego wysłana została wiadomość.

W każdym jednak przypadku, niezależnie od tego, czy użytkownikowi wykonującemu określone działania przypisany został *nick*, czy też nie, system informatyczny obsługujący daną usługę lub serwis rejestruje publiczne numery IP komputerów, z których dokonywane są wpisy. Nazwa (*nick*) przypisana konkretnemu użytkownikowi pełni zatem rolę dodatkowej informacji ułatwiającej identyfikację użytkownika, którą łatwiej zapamiętać niż numer IP komputera. Ułatwia to prowadzenie ewentualnej wymiany poglądów między użytkownikami np. serwisu informacyjnego, którzy – wskazując na *nick* wypowiadającej się osoby – ustosunkowują się do jej wypowiedzi. Jeżeli usługę czatu, forum dyskusyjnego, listy rankingowej itp. prowadzi dostawca usług internetowych,

który jest zobowiązany do rejestrowania i przechowywania tych danych przez określony czas, to *nick* należy rozumieć jako pewną dodatkową daną osobową obok numeru IP przypisanego użytkownikowi, który z danej usługi korzysta. W przypadku użycia *nicków* w rejestrze ruchu telekomunikacyjnego znajdą się wszystkie informacje dotyczące działań wykonywanych przez danego użytkownika, w tym informacja o adresie IP komputera (publicznym lub prywatnym w zależności od miejsca rejestracji), z którego w danej chwili korzystał. Biorąc powyższe pod uwagę oraz fakt, że numery IP komputera mogą stanowić dane osobowe, również *nick*, co do zasady należy uznać za dane osobowe. Opinię tę podzielił również Sąd Najwyższy, który analizował kwestię używania i ochrony *nicków*, a 11 marca 2008 r. wydał w tej sprawie orzeczenie (sygn. akt II CSK 539/07).

Od sformułowanej wyżej zasady mogą się jednak zdarzać, podobnie jak w odniesieniu do numeru IP, pewne wyjątki, bowiem mogą wystąpić sytuacje, w których nie będzie możliwe zidentyfikowanie osoby, której dany *nick* został przypisany.

2.5. Adres poczty elektronicznej

Zgodnie z art. 6 ustawy, za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

Biorąc pod uwagę powyższą definicję, należy stwierdzić, że informacje w postaci adresów e-mail mogą, ale nie muszą, być danymi osobowymi, ponieważ nie zawsze dotyczą one zidentyfikowanych lub możliwych do zidentyfikowania osób. Jako przykład można podać adres e-mail infolinii obsługiwanej przez zespół osób, biur i sekretariatów, gdzie nie są istotne dane osobowe personelu, lecz wyłącznie rola czy charakter wskazanego podmiotu w znaczeniu wyłącznie organizacyjnym, a nie osobowym.

Wobec powyższego warto pokusić się o próbę usystematyzowania tej klasyfikacji i próbę określenia, kiedy posiadając określony adres e-mail rzeczywiście mamy do czynienia z danymi osobowymi, a kie-

dy nie. Mimo usilnych prób rozgraniczenia, nie udaje się jednoznacznie rozstrzygnąć tej kwestii tylko na podstawie treści adresu e-mail. W wielu bowiem adresach e-mail znacząca treść informacyjna zawarta jest w pierwszym członie adresu wskazującym unikalną nazwę użytkownika w ramach obsługiwanych przez dany serwer pocztowy kont pocztowych. Można z dużym prawdopodobieństwem przypuszczać, że nazwy tego członu typu: infolinia, sekretariat, biuro, serwis itp. odnoszą się nie do konkretnych osób fizycznych, lecz podmiotów niebędących nimi. Innym źródłem informacji, o klasyfikacji danego adresu może być, źródło jego pozyskania, czy też inne informacje np. kategorie spraw, w jakich pod dany adres należy przesyłać korespondencję. Podobnie na podstawie tej części nazwy adresu można wnioskować, że dany adres należy do osoby fizycznej. Nie powinno np. budzić wątpliwości, że adres, którego pierwszy człon ma nazwę typu Monika.kowalska, Robert.nowak itp., wskazuje najprawdopodobniej osobę fizyczną. Wątpliwości tej nie będzie również wtedy, gdy adres e-mail otrzymamy od osoby prywatnej, która kontaktując się z nami, przekazała go w celach wymiany korespondencji lub wpisany on został na formularzu np. zgłoszenia konkursowego wysłanego w związku z prowadzoną akcją promocyjną. W przewodniku ochrony danych w Internecie będącym załącznikiem do Rekomendacji Nr R 99 (5) Komitetu Ministrów Rady Europy z 23 lutego 1999 r. dotyczącej ochrony prywatności w Internecie w punkcie 6 części dla użytkowników wskazano wprost: *Pamiętaj, że twój e-mail jest daną osobową i że inni mogą chcieć wykorzystać go do różnych celów, takich jak włączenie do spisu adresowego lub listy użytkowników.*

Innym zagadnieniem jest ocena, czy posiadając adres poczty elektronicznej, co do którego istnieje pewność, że należy do osoby fizycznej, można określić jej tożsamość. W celu rozstrzygnięcia tych wątpliwości należy wziąć pod uwagę wszystkie możliwości (techniczne, organizacyjne i prawne), jakie istnieją w zakresie ustalenia tożsamości osoby, której dotyczy dany adres e-mail. Trzeba mieć również na uwadze fakt, że adres poczty elektronicznej, dla którego w danej chwili nie można ustalić tożsamości osoby, do której on należy, po pewnym czasie stanie się adresem łatwo rozpoznawalnym i ta tożsamość może być bez trudu ustalona.

Kiedy adresy poczty elektronicznej można uznać za dane osobowe

Za dane o charakterze osobowym należy z całą pewnością uznać wszystkie adresy poczty elektronicznej osób fizycznych, które wykupiły konto e-mail u usługodawcy, podpisując stosowną umowę na świadczenie takiej usługi. Tym bardziej wtedy, gdy w identyfikatorze adresu e-mail znajduje się jej imię i nazwisko lub dodatkowo osoba ta wykupiła nazwę domenową niosącą informację o jej nazwisku, np. imię@nazwisko.pl. Operator serwera pocztowego dysponuje w takich przypadkach pełną informacją o tym, do kogo dany adres poczty elektronicznej został przyporządkowany.

Do danych o charakterze osobowym należy również zaliczyć adresy poczty elektronicznej, które nadawca opatrzył swoim zaufanym certyfikatem niekwalifikowanym lub zawarł w nim dokumenty podpisane swoim zaufanym certyfikatem kwalifikowanym.

Należy pamiętać, że usługodawcy oferujący darmowe adresy e-mail dla użytkowników sieci globalnej Internet w przeważającej większości nie nadają procesowi rejestracji konta charakteru formalnego. Taki stan rzeczy sprawia, że użyte mechanizmy automatycznego ich zakładania nie weryfikują faktycznej relacji między osobą tworzącą konto poczty elektronicznej a danymi podanymi przez nią podczas rejestracji tego konta. Nie oznacza to jednak, że adresy tak tworzone nie będą nigdy danymi osobowymi. Patrząc na zakres danych, który można podać przy rejestracji konta, użytkownik sieci Internet, wpisując tam prawdziwe swoje dane osobowe, tworzy adres, do którego jednoznacznie będą przyporządkowane dane identyfikujące jego tożsamość. Z adresem e-mail, który posiada cechy danych osobowych, mamy do czynienia tym bardziej wtedy, kiedy użytkownik, będąc osobą o dość oryginalnym imieniu i nazwisku, zawrze je w identyfikatorze konta (ciągu znaków poprzedzających znaczek @). Nie należy również zapominać o sytuacji, w której osoba rejestrująca adres e-mail, posługuje się nim stale (tak jak numerem telefonu), korzystając z niego w dłuższym okresie i publikuje go przy użyciu różnych mediów wraz ze swoimi danymi osobowymi.

Mimo podania przykładów obiektywnej kwalifikacji osobowego charakteru adresu poczty elektronicznej, każdą sprawę takiej kwalifikacji należy traktować indywidualnie, uwzględniając przedstawione wyżej uwagi.

3. Podatność sieci telekomunikacyjnych na zagrożenia dla bezpieczeństwa informacji

Głównymi czynnikami stwarzającymi zagrożenie dla poufności i integralności danych przetwarzanych w sieciach telekomunikacyjnych, w tym głównie w sieci Internet, są jawność przesyłanych danych oraz łatwość dostępu do nich przez osoby nieuprawnione. Jest to spowodowane publicznym charakterem wykorzystywanej infrastruktury (łącza kablowe i światłowodowe) oraz publiczną dostępnością medium (w przypadku wykorzystywania łączności radiowej). Publiczny dostęp do istniejącej infrastruktury sieci telekomunikacyjnych nie tylko w obrębie kraju, ale niemal całej społeczności na świecie wynika z naturalnych potrzeb komunikowania się oraz wymiany informacji, którymi społeczność chce się dzielić i które nie podlegają żadnym ograniczeniom.

3.1. Jawność danych w czasie transmisji

Sieć Internet w swojej pierwotnej postaci zaprojektowana została przede wszystkim dla potrzeb wymiany informacji w środowisku akademickim. Nie przewidywano wówczas, że będzie ona wykorzystywana również przez inne środowiska i że sprawa ochrony poufności przekazywanych informacji stanie się dla określonych zastosowań zagadnieniem kluczowym. Jej twórcy koncentrowali się na zapewnieniu mechanizmów kontroli i korekcji naturalnych błędów transmisji powodowanych fizycznymi zakłóceniami sygnałów przesyłanych w sieci, nie poświęcając wystarczającej uwagi zapewnieniu poufności przesyłanych danych czy też innym mechanizmom kontroli dostępu przeciwdziałającym celowym nadużyciom użytkowników. Podstawowym standardem wymiany da-

nych, jaki został przez nich wypracowany do przesyłania danych między poszczególnymi komputerami, jest używany do dziś standard TCP/IP (*Transmission Control Protocol* – protokół kontroli transmisji/Internet Protocol – protokół internetowy) nazywany również protokołem[11] TCP/IP. Jego główną zaletą była otwartość, tj. możliwość komunikacji między dowolnymi typami urządzeń, bez względu na ich fizyczną różnorodność. Ta cecha spowodowała, że protokół ten przetrwał do dziś i stosowany jest nie tylko do przesyłania danych między komputerami, ale również między innymi urządzeniami telekomunikacyjnymi, takimi jak terminale płatnicze, telefony, drukarki, kamery i inne urządzenia specjalistyczne. Protokół TCP/IP, a w zasadzie para protokołów TCP i IP, stosowany jest odpowiednio do kontroli i transportu danych. Protokół IP służy do przesyłania dowolnych danych z punktu do punktu zaś TCP do uzgadniania tożsamości, zarządzania pakietami danych (mogą docierać do adresata w innej kolejności niż były wysłane), sterowania ich transportem i wykrywania oraz obsługi błędów.

Protokoły TCP/IP nie zawierają mechanizmów zabezpieczenia przesyłanych w sieci pakietów danych przed podglądem osób nieupoważnionych. Dane przesyłane zgodnie z protokołem IP zapisane są w przekazywanym pakiecie danych w postaci jawnej (nieszyfrowanej). Mechanizmy adresacji, służące kontroli nadawcy i odbiorcy, nie są odporne na ataki. Właściwości te sprawiają, że przesyłane informacje narażone są na niebezpieczeństwo utraty poufności, co w przypadku choćby informacji o identyfikatorach i hasłach dostępu do systemów informatycznych, kont bankowych itp. może spowodować ogromne, często trudne do oszacowania straty.

Wskazana jawność transportu danych w protokole TCP/IP skutkuje przenoszeniem tej cechy do innych protokołów komunikacyjnych, których funkcjonowanie bazuje na protokole TCP/IP, np. takich jak protokół SMTP (*Simple Mail Transfer Protocol*) do obsługi poczty elektronicznej, HTTP (*Hypertext Transfer Protocol*) do przesyłania i udo-

[11] Protokół TCP/IP oraz inne protokoły stosowane w Internecie do wymiany informacji to zbiory ścisłych reguł postępowania, które są automatycznie wykonywane przez urządzenia w celu nawiązania łączności i wymiany danych.

stępniania dokumentów hipertekstowych w procesie komunikowania się ze stronami internetowymi czy też protokół SNMT (*Simple Network Management Protocol*) służący do zdalnego sterowania komputerami, routerami i innymi urządzeniami w sieciach telekomunikacyjnych.

Odpowiednie mechanizmy służące ochronie poufności transportu danych w sieci Internet opracowane zostały w terminie późniejszym na bazie algorytmów kryptografii asymetrycznej. Pierwsze rozwiązanie w tym zakresie w 1994 r. przedstawiła firma Netscape. Stworzyła ona protokół SSL (*Secure Socket Layer*) służący do bezpiecznej transmisji zaszyfrowanego strumienia danych. W 1996 r. międzynarodowa organizacja *Internet Engineering Task Force* (IETF) powołała grupę roboczą TLS (*Transport Layer Security*), której zadaniem było rozwijanie protokołu SSL. Wynikiem jej prac jest opublikowany w 1999 r. standard TLS 1.0, określany również jako standard (protokół) SSL 3.1. SSL jest rozwiązaniem typu klient-serwer, które oprócz mechanizmów szyfrowania, zapewnia mechanizmy służące uwierzytelnianiu serwerów, z którymi następuje połączenie. Protokoły SSL/TSL nie są jednak powszechnie stosowane, co sprawia, że poufność danych transportowanych poprzez sieć publiczną nie zawsze jest zapewniona.

3.2. Korzystanie z sieci publicznych

Publiczna dostępność usług telekomunikacyjnych, a głównie fakt współdzielenia tych samych urządzeń przesyłowych (łączy telekomunikacyjnych, urządzeń sieciowych typu routery, przełączniki) przez różne podmioty, to słaby punkt bezpieczeństwa usług sieciowych. Duże zalety sieci Internet, jakimi są możliwość komunikowania się z bardzo liczną społecznością czy publicznego udostępniania różnorodnych treści i produktów informatycznych, np. programów i gier, stały się jednocześnie jej bardzo poważnym zagrożeniem, a sieć bywa wykorzystywana nie tylko w szlachetnych celach.

W sieci udostępnianych jest wiele informacji, a także narzędzi programowych, które mogą być wykorzystane w różnych celach. Publikowanie rozkładów jazdy, godzin pracy urzędów, przepisów obo-

wiązującego prawa, materiałów dydaktycznych i naukowych, różnego typu instrukcji, wskazówek itp. to przykłady wykorzystania Internetu w pożytecznych celach. Ta sama sieć może jednak być wykorzystywana do publikowania materiałów uznawanych powszechnie za szkodliwe, bo dotyczą przemocy, pornografii, nawoływania do działań przestępczych itp.

W podobnych kategoriach należy oceniać udostępniane w sieciach, a więc dostępne dla szerokiego kręgu odbiorców, narzędzia programowe. Np. narzędzia do skanowania sieci i śledzenia przepływu danych mogą być wykorzystywane zarówno przez ich administratorów dla identyfikacji słabych punktów zabezpieczenia w celu ich wzmocnienia, jak również przez przestępców w celu uzyskania nieuprawnionego dostępu.

3.3. Bezprzewodowe kanały komunikacyjne

Dodatkowym czynnikiem zwiększającym zagrożenia dla bezpieczeństwa systemów informatycznych i sieci telekomunikacyjnych jest coraz powszechniej stosowana łączność bezprzewodowa. Jej charakterystyczną cechą jest to, że przesyłane przy użyciu tego medium dane mogą być odczytane na urządzeniu znajdującym się w określonej odległości od źródła sygnału bez konieczności łączenia go z tym źródłem przy użyciu przewodów. W przypadku braku zabezpieczeń kryptograficznych korzystanie z takich sieci stwarza poważne zagrożenie utraty poufności danych. Jako główne źródła zagrożeń w sieciach bezprzewodowych wskazuje się:

- współdzielony charakter wykorzystywanego medium (fale elektromagnetyczne),
- nieefektywność zabezpieczeń fizycznych,
- domyślna konfiguracja zakładająca brak szyfrowania,
- słabość szyfrowania w standardzie WEP, który jest stosowany w wielu urządzeniach mobilnych.

3.4. *Hotspoty*

Szczególnym przypadkiem łączności bezprzewodowej są sieci wykorzystujące fale radiowe do przesyłania danych w standardzie WiFi, umożliwiające nieodpłatny dostęp do usług sieci Internet bez konieczności jakiegokolwiek uwierzytelniania się użytkowników. Obszar zasięgu fal radiowych, gdzie można uzyskać taki dostęp do sieci, nazywa się *hotspotem*. Podstawowym elementem *hotspotu* jest urządzenie o nazwie Punkt Dostępu (*Access Point*), które zapewnia stacjom komputerowym wyposażonym w bezprzewodowy interfejs sieciowy, dostęp do zasobów sieci za pomocą bezprzewodowego medium transmisyjnego.

Sieci bezprzewodowe, w większym stopniu niż sieci „tradycyjne", narażone są na próby włamania, podsłuchu czy kradzieży danych. Nieograniczony dostęp do medium transmisyjnego ma wpływ na poziom bezpieczeństwa zarówno infrastruktury sieciowej *hotspotu*, jak i przesyłanych w niej danych. Nie bez znaczenia dla bezpieczeństwa takich połączeń pozostaje fakt, że wiele urządzeń sieciowych jest gotowych do pracy bezpośrednio po podłączeniu, bez potrzeby konfigurowania zabezpieczeń. Producenci sprzedają urządzenia z domyślnymi ustawieniami w celu ich łatwiejszej instalacji przez użytkownika. Jest to rozwiązanie wygodne dla użytkownika, ale stwarza duże zagrożenia dla bezpieczeństwa całej infrastruktury sieciowej i podłączonego do niej komputera. Większość użytkowników nie stosuje się do zaleceń producentów i nie dokonuje żadnych zmian w konfiguracji urządzenia, co w znacznym stopniu zwiększa ryzyko niekontrolowanego dostępu do sieci przez osoby nieuprawnione.

W przypadku korzystania z *hotspotu* użytkownik może być łatwo wprowadzony w błąd co do rzeczywistego administratora infrastruktury danego *hotspotu* i rzeczywistych intencji jego działania. Dlatego jednym z poważnych zagrożeń bezpieczeństwa informacji w przypadku korzystania z sieci WiFi są tzw. fałszywe *hotspoty*. Przestępcy zakładają tymczasowe bezprzewodowe punkty dostępu do Internetu, aby przechwytywać poufne informacje przesyłane siecią, takie jak loginy i hasła do kont bankowych czy dane z kart kredytowych. Jak ostrzegają specjaliści firmy

RSA Security w swoim raporcie[12] fałszywy *hotspot* można bardzo łatwo zainstalować, a atak przy ich pomocy gwarantuje pozyskanie wartościowych dla przestępców danych w krótkim czasie. Prawdopodobieństwo przechwytywania danych z kart kredytowych przy transakcjach za pośrednictwem *hotspotów* jest relatywnie wysokie.

Żeby przeciwdziałać tym zagrożeniom, mobilni użytkownicy Internetu, tj. osoby korzystające z Internetu przy użyciu komputerów przenośnych (laptopów, palmtopów), telefonów z wbudowanymi interfejsami dostępu do sieci itp., powinni być odpowiednio uświadomieni i przeszkoleni co do potencjalnych zagrożeń wynikających z istnienia fałszywych *hotspotów*. Powinni znać przyczynę wprowadzonych w polityce bezpieczeństwa zakazów wysyłania prawnie chronionych danych poprzez łącza transmisyjne niezapewniające kryptograficznej ochrony danych i przestrzegać je w praktyce.

4. Potrzeby zabezpieczenia poufności

Zagrożenia związane z przetwarzaniem danych osobowych przy użyciu systemów informatycznych w dużej mierze zależą od środowiska, w którym dany system funkcjonuje. Przy czym największe ryzyko utraty poufności występuje wówczas, gdy komputery połączone są ze sobą przy użyciu sieci publicznej. W praktyce można wówczas mówić nie o połączeniu danego komputera z innym lub innymi komputerami, lecz o połączeniu danego komputera z siecią publiczną, do której podłączone są również miliony innych komputerów. Połączenie takie sprawia, że jeżeli dostęp do zgromadzonych na danym komputerze informacji nie będzie odpowiednio ograniczony, to mogą być one narażone na utratę poufności, nieupoważnioną zmianę lub zniszczenie. Ponadto w przypadku zdalnego korzystania z takiego komputera (odczytywanie, zmiana lub zapis zgromadzonych tam informacji) odpowiednich zabezpieczeń wy-

[12] http://www.rsa.com/press_release.aspx?id=6870; RSA Security; „Wireless Adoption Increases, Security Improves in World's Major Cities"; Press Releases; Thursday, May 25, 2006.

magają kanały komunikacyjne między urządzeniem dostępowym (stacja komputerowa użytkownika) a komputerem, na którego nośnikach informacje te są przechowywane.

System informatyczny pracujący w środowisku sieciowym, zwłaszcza w środowisku sieci publicznej, jakim jest sieć Internet, musi być chroniony zarówno przed atakami pochodzącymi od wewnątrz, tj. od nielojalnych współpracowników, jak i z zewnątrz. Ochronie muszą podlegać nie tylko przetwarzane w nim dane osobowe i inne informacje podlegające ochronie, ale również sam system użyty do ich przetwarzania. Dane w systemie informatycznym mogą być bowiem przetwarzane albo przy użyciu specjalnych programów, albo innych, uniwersalnych narzędzi programowych, takich jak edytor tekstu, edytor bazy danych itp.

Utrzymanie bezpieczeństwa systemu pracującego w środowisku sieciowym jest szczególnie trudne. Wynika to stąd, że administrator odpowiedzialny za zabezpieczenie danych w takim środowisku jest – w porównaniu z atakującymi – na z góry straconej pozycji.

Żeby bowiem skutecznie zabezpieczyć system należy usunąć „wszystkie" jego słabości i podatność na znane rodzaje ataków, jak również ataki, które mogą pojawić się w najbliższej przyszłości, zaś aby skutecznie zaatakować – wystarczy znaleźć jedną słabość danego systemu i stosownie ją wykorzystać.

Ponadto analizując ochronę sytemu połączonego z siecią publiczną, jaką jest sieć Internet, trzeba zwrócić uwagę na fakt, że system ów jest „widoczny" dla milionów użytkowników z całego świata. Potrzeba połączenia z Internetem wynika bardzo często z potrzeb dostępności danego systemu dla wielu użytkowników, niezależnie od miejsca, w którym się znajdują. Nie oznacza to jednak, że system taki ma być dostępny dla wszystkich, którzy go „widzą". System taki, jak również przetwarzane w nim informacje, powinny być dostępne tylko dla osób, które mają stosowne uprawnienia. Dla pozostałych osób (użytkowników sieci Internet), które nie posiadają upoważnień, system ten powinien być niedostępny. Biorąc pod uwagę proporcje liczby

osób, dla których system i przetwarzane w nim dane powinny być niedostępne, do liczby osób, dla których powinny być udostępnione, znaczenie właściwych zabezpieczeń jest szczególne.

Należy mieć na uwadze fakt, że: **Przy połączeniu systemu z siecią publiczną, jaką jest sieć Internet, nad zabezpieczeniem systemu w sieci czuwa najczęściej jedna, a najwyżej kilka osób, podczas gdy nad złamaniem zastosowanych zabezpieczeń mogą pracować tysiące osób z różnych miejsc na całym świecie.**

5. Narzędzia programowe wykorzystywane do ataku na bezpieczeństwo informacji

Do wspomagania ataku na bezpieczeństwo danych może być użytych wiele różnych metod i narzędzi. Do najbardziej znanych i typowych narzędzi wykorzystywanych do działań na szkodę bezpieczeństwa informacji można zaliczyć narzędzia programowe, takie jak: wirusy komputerowe, robaki, trojany, *backdory, rootkity, keyloggery* programowe, *spyware*, *exploity*, *dialery* oraz narzędzia sprzętowe, takie jak: *keyloggery* sprzętowe, czytniki kart, kamery, urządzenia podsłuchowe.

5.1. Wirusy komputerowe

Wirusy komputerowe to programy celowo zaprojektowane do zakłócania pracy komputera, rejestrowania, uszkadzania lub usuwania danych. Ich charakterystyczną cechą jest możliwość łatwego rozprzestrzeniania się do innych komputerów poprzez „przyklejanie się" do innych plików (wirusy plikowe) lub „zagnieżdżanie się" na zerowej ścieżce dysku lub dyskietki poprzez modyfikacje struktury zapisu danych (wirusy dyskowe).

Wirusy komputerowe można podzielić według wielu kryteriów. Ze względu na infekowany obiekt wirusy dzieli się na:

- dyskowe – infekujące sektory startowe dyskietek i dysków twardych,
- plikowe, które infekują pliki wykonywalne[13] danego systemu operacyjnego,
- skryptowe, które bazują na wykorzystaniu języków skryptowych systemu operacyjnego lub języków skryptowych interpreterów[14], takich jak java script, visual basic, php i inne,
- makrowirusy, których kod składa się z instrukcji w języku wysokiego poziomu, wykonywane przez interpreter,
- komórkowe, infekujące oprogramowanie telefonów komórkowych i dostępne poprzez nie usługi.

Technologia wirusów i metody ich działania zmieniają się w ślad za wprowadzaniem i rozwojem nowych technologii w architekturach budowy komputerów i sieci komputerowych. Wirusy dyskowe były np. bardzo popularne w okresie, kiedy powszechne było kopiowanie danych i programów przy użyciu dyskietek. Wirusy te przenosiły się między komputerami za pośrednictwem dyskietek, na których zmieniały strukturę zapisu informacji i/lub kopiowanych plików zawierających programy. Dyskietki takie odczytywane w środowisku nieposiadającym odpowiednich zabezpieczeń zarażały pliki wykonywalne danego systemu, a następnie kolejne dyskietki. Możliwości ich rozprzestrzeniania się zostały znacznie ograniczone z czasem, kiedy dyskietki zostały wyparte przez CD ROM-y, a źródłem

[13] Plik wykonywalny to plik programu w postaci, która pozwala na jego uruchomienie bezpośrednio w środowisku systemu operacyjnego komputera. Plik wykonywalny zawiera instrukcje programu zapisane bezpośrednio w języku procesora danego komputera. Wykonanie poleceń zawartych w pliku wykonywalnym nie wymaga interpretacji do postaci poleceń procesora.

[14] Interpreter to program komputerowy, który analizuje polecenia programu zapisane w języku programowania używanym przez programistę i wykonuje przeanalizowane fragmenty. W przeciwieństwie do kompilatora, który analizuje polecenia programu zapisane w języku programisty i tworzy plik zawierający polecenia gotowe do późniejszego wykonania przez procesor komputera, interpreter czyni to bezpośrednio, odczytując i interpretując kolejne polecenia.

pozyskiwania wielu informacji i narzędzi programowych stał się Internet. Dzisiaj w swej pierwotnej postaci są one praktycznie niespotykane.

Najnowszą generację wirusów stanowią wirusy infekujące nie tylko komputery, ale również telefony komórkowe wyposażone w system operacyjny (tzw. *smartfony*) oraz inne urządzenia przenośne. Rozprzestrzeniają się one głównie poprzez sieć za pomocą wiadomości typu MMS, ściąganych plików, załączników do wiadomości poczty elektronicznej, komunikatorów typu Gadu-Gadu, IRC i wielu innych.

Wirusy komputerowe mogą być łagodne lub złośliwe. Te łagodne powodują tylko utrudnianie pracy, np. spowalniają pracę komputera, wyświetlają grafikę, odgrywają dźwięki, wyłączają komputer, blokują niektóre usługi itp. Te złośliwe zaś mogą wyrządzić znacznie poważniejsze szkody. Wirusy złośliwe mogą „otworzyć" nieuprawnionym osobom dostęp do przetwarzanych na danym komputerze informacji, w tym informacji prawnie chronionych, takich jak dane osobowe, numery kart kredytowych itp. W innych przypadkach wirusy złośliwe mogą wysłać wyszukane na zarażonym komputerze dane na wskazany adres przestępcy komputerowego w celu ich nieuprawnionego użycia lub odsprzedania na czarnym rynku. Zainfekowane złośliwymi wirusami komputery mogą rozsyłać spam lub być użyte do ataku na inne komputery w sieci.

5.2. Robaki

Robaki komputerowe to samopowielające się programy komputerowe, podobne do wirusa komputerowego. Główną różnicą między wirusem a robakiem jest to, że robak nie potrzebuje nosiciela – zwykle jakiegoś pliku będącego programem, który modyfikuje, doczepiając do niego kod swojego programu. Robak jest pod tym względem samodzielny, a rozprzestrzenia się we wszystkich sieciach podłączonych do zarażonego komputera poprzez wykorzystanie luk w systemie operacyjnym lub nieostrożność i brak świadomości użytkownika. Oprócz mechanizmów zapewniających samopowielanie się, robak może mieć wbudowane procedury dodatkowe, takie jak niszczenie plików, wysyłanie poczty (z reguły *spam*) lub pełnienie roli *backdoora* bądź konia trojańskiego. Współczesne robaki potrafią uzupełniać

i zmieniać swoją funkcjonalność, pobierając z sieci dodatkowe moduły programowe. Niektóre robaki posiadają również możliwość zdalnego sterowania dalszym działaniem zainfekowanego komputera, w tym łączenia zainfekowanych komputerów w sieci, tzw. *botnety*[15] używane przez przestępców do prowadzenie zmasowanych akcji wysyłania spamu lub przeprowadzenia ataku typu DDoS[16]. Robaki najczęściej dystrybuowane są za pomocą poczty elektronicznej w postaci tzw. *downloaderów*, tj. programów łączących komputer klienta z komputerem, na którym udostępniony jest kod robaka w celu jego pobrania, względnie prostych i małych programów, których jedynym zadaniem jest skomunikowanie się z „centrum operacyjnym" (np. za pomocą kanału IRC) i pobranie dodatkowych modułów programowych.

5.3. Trojany

Trojany to programy, które – podszywając się pod przydatne lub ciekawe dla użytkownika aplikacje – dodatkowo implementują niepożądaną, ukrytą przed użytkownikiem funkcjonalność. Trojany zainstalowane na komputerze ofiary umożliwiają przestępcom zdalny dostęp do zapisanych na nim danych oraz zarządzanie nim. Do najpopularniejszych szkodliwych działań, jakie mogą być wykonywane przy użyciu trojanów, należą:

[15] *Botnet* – grupa komputerów zainfekowanych złośliwym oprogramowaniem (np. robakiem) pozostającym w ukryciu przed użytkownikiem i pozwalającym przestępcom na sprawowanie zdalnej kontroli nad tymi komputerami. Pojedynczy komputer w takiej sieci nazywany jest komputerem zombie. Obecnie całkowitą liczbę komputerów zombie na świecie szacuje się na kilka milionów – liczba ta systematycznie wzrasta.

[16] DDoS (ang. *Distributed Denial of Service*) – atak na system komputerowy lub usługę sieciową przeprowadzany równocześnie z wielu komputerów (np. zombie) w celu uniemożliwienia działania poprzez zajęcie wszystkich wolnych zasobów. Atak DDoS jest odmianą ataku DoS polegającą na jednoczesnym atakowaniu ofiary z wielu miejsc. Służą do tego najczęściej komputery, nad którymi przejęto kontrolę przy użyciu specjalnego oprogramowania (różnego rodzaju tzw. boty i trojany). Na dany sygnał komputery zaczynają jednocześnie atakować system ofiary, zasypując go fałszywymi próbami skorzystania z usług, jakie oferuje. Dla każdego takiego wywołania atakowany komputer musi przydzielić pewne zasoby (pamięć, czas procesora, pasmo sieciowe), co przy bardzo dużej ilości żądań prowadzi do wyczerpania dostępnych zasobów, a w efekcie do przerwy w działaniu lub nawet zawieszenia systemu.

- instalowanie w systemie programu umożliwiającego nielegalny dostęp (*backdoora*) i umożliwienie kontroli nad systemem osobom trzecim w celu np. rozsyłania spamu, dokonywania ataków typu DDoS itp.,
- szpiegowanie i wykradanie poufnych danych użytkownika (*spyware*),
- utrudnianie pracy programom antywirusowym,
- zmienianie strony startowej przeglądarki www w celu zaprezentowania reklamy,
- działania destrukcyjne (kasowanie plików, uniemożliwianie korzystania z komputera poprzez usunięcie plików systemowych czy też zaszyfrowanie ważnych plików z danymi w celu wyłudzenia okupu za dostarczenie klucza do ich odzyskania).

Wszystkie trojany składają się z dwóch plików, z których jeden jest serwerem, a drugi klientem. Plik serwera zainstalowany na komputerze ofiary umożliwia zdalne zarządzanie tym komputerem, w tym wgląd w zapisane na nim dane. Do najbardziej znanych trojanów należą NetBus i CAFEiNi.

Atakujący trojanem może dołączyć do wiadomości e-mail niewinnie wyglądający plik, który zachęca użytkownika do uruchomienia. Trojan jest z reguły plikiem wykonywalnym, tj. programem, i dlatego musi mieć rozszerzenie nazwy typowe dla pliku wykonywalnego, tzn. takie jak .exe, .com, .scr, .bat, lub .pif. Na platformie Microsoft Windows skonfigurowanej tak, aby ukrywać rozszerzenie, plik trojana nazwany np. „readme.txt.exe" będzie widoczny jedynie pod nazwę „readme.txt" i użytkownik uzna go za nieszkodliwy plik tekstowy. Kiedy odbiorca e-maila uruchomi załącznik, trojan może wykonać jakąś pozorną operację, której spodziewa się użytkownik (np. otworzy plik tekstowy), tak aby ofiara pozostała nieświadoma niszczycielskiego działania trojana. W tym samym czasie trojan może modyfikować lub kasować pliki, zmieniać konfigurację komputera, zebrać wszystkie zidentyfikowane na danym komputerze poufne dane, takie jak dane osobowe, numery kart kredytowych, adresy poczty elektronicznej i wysłać na wskazany adres

przestępcy, a nawet używać komputera jako bazy (zombi), z której atakowana jest sieć lokalna lub inne sieci.

5.4. *Backdory*

Backdoory (ang. tylne drzwi) to luki w zabezpieczeniach systemu utworzone umyślnie w celu późniejszego wykorzystania. *Backdoor* w systemie może być np. wykonany przez osobę, która włamała się przez inną lukę w oprogramowaniu (której przydatność jest ograniczona czasowo do momentu jej usunięcia) bądź poprzez podrzucenie użytkownikowi trojana. Osoba taka, uzyskawszy dostęp do zarządzania systemem, wprowadza w nim takie zmiany konfiguracyjne (tylne drzwi), np. tworzy tajne konto z uprawnieniami administratora, które umożliwiają jej późniejsze zarządzanie systemem lub śledzenie wykonywanych w nim operacji. *Backdoor* może być również umyślnie utworzony przez twórcę danego systemu w celu umożliwienia sobie w przyszłości dostępu do niego bez wiedzy jego przyszłego właściciela. Czynność taka jest szczególnie łatwa wtedy, gdy użytkownik nie ma wglądu do kodu źródłowego danego systemu, czyli kodu zapisanego w jednym z języków programowania wyższego poziomu, z którego analizy łatwo można byłoby odczytać kolejne działania wykonywane przez system.

5.5. *Rootkity*

Rootkity to narzędzia pomocne we włamaniach do systemów informatycznych. Ukrywają one niebezpieczne pliki i procesy, które umożliwiają utrzymanie kontroli nad systemem. *Rootkity* infekują jądro systemu i wprowadzają w nim takie zmiany, które powodują, że wywołane przez nie procesy nie są widoczne przez użytkownika ani inne programy, np. programy antywirusowe. Ich działanie powoduje ukrywanie reprezentujących je procesów z listy procesów systemu oraz plików, w których są przechowywane z listy, plików w API[17] systemu operacyjnego.

[17] API (ang. *Application Programming Interface*) — specyfikacja procedur, funkcji lub interfejsów umożliwiających komunikację z daną aplikacją systemem operacyjnym lub innym systemem zewnętrznym umożliwiająca stosowanych bibliotek programowych do komunikacji z innymi aplikacjami.

Poprzez takie modyfikacje systemu *rootkit* może np. ukryć siebie oraz trojana przed administratorem oraz oprogramowaniem antywirusowym. Ukrywanie odbywa się najczęściej przez przejęcie wybranych funkcji systemu operacyjnego służących np. listowaniu procesów lub plików w katalogu, a następnie „cenzurowaniu" zwracanych przez te funkcje wyników tak, by ukrywane przez *rootkit* nazwy nie znajdowały się na liście wynikowej. Zaatakowany *rootkitem* system zachowuje się jak system w pełni zabezpieczony. Standardowe oprogramowanie antywirusowe nie wykrywa żadnych objawów infekcji. Specjaliści twierdzą, że *rootkity* nie są czymś nowym. Były stosowane już wcześniej w systemach serwerowych. Teraz jednak ich zastosowanie przenosi się na systemy komputerowe użytkowników domowych. Do wykrywania obecności rootkitów stosowane są specjalne narzędzia programowe. W ostatnim okresie, ze względu na narastającą inwazję tego typu oprogramowania złośliwego, również producenci oprogramowania antywirusowego rozszerzają funkcjonalność swoich produktów o możliwości wykrywania i usuwania *rootkitów*.

5.6. *Keyloggery*

Keyloggery to sprzętowe lub programowe moduły, które zainstalowane na komputerze użytkownika (ofiary) potrafią odczytać i przechować w pamięci historię wciśniętych przez niego klawiszy. W ten sposób mogą służyć do przechwycenia stosowanych przez użytkownika danych służących do uwierzytelnienia się (np. identyfikatorów i haseł) oraz innych danych wprowadzanych do komputera.

Keyloggery programowe to programy, które działają na zasadzie przejęcia kontroli nad procedurami systemu operacyjnego służącymi do obsługi klawiatury. Każde wciśnięcie klawisza jest odnotowywane w specjalnym pliku, który ukrywany jest przed użytkownikiem np. w katalogach systemowych. Opcjonalnie informacje o wciśniętych klawiszach poszerzane są o dodatkowe informacje, jak nazwa aktywnego programu lub okna, w celu łatwiejszej identyfikacji kontekstu, w jakim wpisywane były zarejestrowane znaki. Większość *keyloggerów* ma spe-

cjalnie stworzoną funkcję, która pozwala na wysłanie pliku z hasłami na wyznaczony adres pocztowy przestępcy.

Keyloggery sprzętowe mogą mieć postać małych przejściówek służących do wpięcia do portu klawiatury komputera lub układu wbudowanego w kabel łączący klawiaturę z komputerem. Układy takie mogą być wbudowane również w klawiaturę. W przypadku *keyloggerów* – przejściówek, klawiaturę wpina się do gniazda w przejściówce. Wszystkie znaki wpisywane z klawiatury, a także sygnały sterujące z systemu, przechodząc przez taką przejściówkę, są odpowiednio przetwarzane. Wstawienie takiego układu na drodze sygnału od klawiatury do odpowiedniego portu wejściowego komputera jest całkowicie niewidoczne dla systemu operacyjnego komputera i czuwających nad bezpieczeństwem komputera programów zabezpieczających typu antywirusy, *antyrootkity*, *firewalle* itp. Układy wbudowane w *keyloggery* sprzętowe mają moduł pamięci, w którym zapisywane są wszystkie znaki, jakie użytkownik wprowadza, komunikując się z komputerem, lub układ wysyłający te znaki drogą radiową do odbiorcy.

Keyloggery są narzędziami, które mogą być stosowane zarówno przez przestępców do kradzieży danych, w tym tzw. kradzieży tożsamości elektronicznej użytkowników (loginów, haseł, numerów PIN itp.), jak i administratorów w celach wykrycia nieuprawnionego korzystania z komputerów. Producenci tych narzędzi w ofertach sprzedaży reklamują je jako pożyteczne narzędzia do monitoringu komputera. Np. jedna z firm zajmujących się dystrybucją *keyloggerów KeyShark* przedstawia je jako pożyteczne narzędzia służące do wykrywania:

- oszustw komputerowych,
- nieautoryzowanego dostępu do komputera (np. w domu, w firmie),
- niewłaściwego użycia komputera przez pracownika w przedsiębiorstwie,
- nieodpowiedniego użycia komputera przez dzieci,
- jak również do archiwizacji danych w czasie rzeczywistym, co może ochronić przed utratą efektów wielogodzinnej pracy.

Keyloggery stanowią nie tylko poważne zagrożenie dla sekretów i prywatności użytkownika. Mogą też być użyte do kradzieży elektronicznej tożsamości użytkownika w postaci haseł do kont bankowych, skrzynek pocztowych, numerów kart kredytowych itp. Skutki takich działań dla poszkodowanego użytkownika mogą być bardzo dotkliwe ekonomicznie. Jako przykład niech posłuży sprawa Joe Lopeza[18], biznesmena z Florydy, który w lutym 2005 r. wytoczył proces przeciwko Bank of America, po tym jak z jego konta w tym banku nieznani sprawcy ukradli i przetransferowali na terytorium Łotwy 90 000 dolarów. Przeprowadzone śledztwo wykazało wówczas, że komputer Lopeza został zainfekowany szkodliwym programem o nazwie Backdoor.Coreflood, który rejestruje każde uderzenie klawisza i poprzez Internet wysyła te informacje przestępcom komputerowym. Lopez często wykorzystywał Internet do zarządzania swoim kontem w Bank of America i jego dane trafiły w ten sposób w ręce przestępców. Sąd stwierdził, że Lopez nie zastosował podstawowych środków bezpieczeństwa podczas zarządzania swoim kontem w Internecie i nie przyznał mu żadnego odszkodowania od banku. Po tym zdarzeniu w 2003 r. sygnatura *keyloggera* Backdoor.Coreflood została dodana do baz prawie wszystkich produktów antywirusowych. Podobnych przykładów można podać więcej, np. okradzenie w 2006 r. klientów banków brazylijskich na łączną kwotę około 4,7 mln dolarów[19], a banków francuskich na około 1 mln euro[20].

5.7. *Spyware*

Spyware – inaczej oprogramowanie szpiegujące – to rodzaj oprogramowania, które umieszczone na komputerze użytkownika w sposób

[18] http://www.viruslist.pl/analysis.html?newsid=422#res; Nikolay Grebennikov; „Keyloggery: Jak działają i jak można je wykryć (część 1)".

[19] http://www.nytimes.com/2006/02/27/technology/27hack.html?_r=2, Tom Zeller Jr; Cyberthieves Silently Copy Your Passwords as You Type; Luty, 27, 2006 r.

[20] http://www.guardian.co.uk/technology/2006/feb/07/news.france; Kim Willsher; "Sleeper bugs used to steal €1m in France", The Guardian, Tuesday, 7 February 2006 r.

przez niego niedostrzegany umożliwia zbieranie informacji o nim, jego zainteresowaniach, najczęściej odwiedzanych stronach internetowych itp. oraz przekazywanie tych informacji zainteresowanym firmom, przeważnie na potrzeby podjęcia działań marketingowych, które zasypują potem użytkowników spamem reklamowym. Dobrze jednak, jeśli następstwem będzie tylko uciążliwy spam. W ostatnim czasie wśród programów szpiegowskich znajdują się również takie, które zdolne są przechwycić sesję użytkownika podczas pracy przeglądarki, tzw. *browser hijacking* (porywanie przeglądarki) oraz przejąć nadzór nad uruchomionym procesem, np. wykonywaniem operacji bankowej.

Oprogramowanie typu *spyware* najczęściej jest dodatkowym i ukrytym komponentem większego programu. Modułów *spyware* nie można usunąć np. poprzez typowe odinstalowanie aplikacji, której instalacja spowodowała ich wprowadzenie do systemu. Oprogramowanie *spyware* zmienia często wpisy do rejestru systemu operacyjnego i ustawienia użytkownika. Potrafi pobierać i uruchamiać pliki ściągnięte z sieci. Ofiarami działań *spyware* stają się najczęściej osoby, które bezpłatnie pobierają z Internetu potrzebne im aplikacje typu *adware* i *freeware*. Niestety, zapominają one przy tym, że nie ma nic za darmo. Autorzy programów typu *adware* i *freeware* też muszą zarabiać i robią to, współpracując z firmami zbierającymi informacje o naszych zainteresowaniach. W instalatorze takich aplikacji może być ukryty moduł, który dodaje do systemu komputerowego użytkownika niewielki program zbierający odpowiednie dane. Program ten, jak już wspomniano, pozostaje często w komputerze użytkownika nawet wtedy, gdy użytkownik usunie aplikację, podczas instalacji której został on wprowadzony.

5.8. *Exploity*

Exploity to programy, których celem jest wykorzystanie błędów wykrytych w systemie operacyjnym komputera, jego oprogramowaniu systemowym lub luki w zabezpieczeniach mające na celu przejęcie nad nim kontroli lub wykonanie określonych operacji na jego zasobach. *Exploit* za pomocą odpowiednio przygotowanego kodu wykorzystu-

je błąd programistyczny występujący w oprogramowaniu komputera w celu przejęcia kontroli nad działaniem całego systemu operacyjnego komputera lub wybranego procesu. Powoduje on najczęściej uruchomienie tych procesów danego systemu, które odpowiedzialne są za sterowanie uprawnieniami i kontrolę pracy innych modułów, co stwarza szerokie możliwości wykonywania operacji w danym systemie przez nieuprawnione osoby. Wytworzenie *exploita* wymaga odpowiedniej wiedzy z zakresu inżynierii oprogramowania. Gotowe zaś *exploity* mogą być użyte przez osoby bez jakiejkolwiek wiedzy programistycznej tzw. *script kiddies* (skryptowych dzieciaków, skrypciarzy – osoby, których wiedza ogranicza się do sposobu użycia danego *exploita* i wykorzystania wyników jego działania). Osoby takie korzystając z gotowych *exploitów* umieszczanych w sieci, mogą przeprowadzić skuteczne, często bardzo szkodliwe w skutkach ataki na systemy komputerowe.

W odpowiedzi na ujawnione błędy w oprogramowaniu lub wytworzone już *exploity* autorzy systemu bądź aplikacji opracowują odpowiednie programy naprawcze, których zadaniem jest usunięcie wykrytego błędu poprzez wprowadzenie odpowiednich uzupełnień. Uzupełnienia te, nazywane *hot fix* lub *patch* (łata), tworzone są po to, aby naprawić wykryte błędy lub luki w zabezpieczeniach danego systemu. Uzupełnienia te umieszczane są zazwyczaj na stronach internetowych producentów oprogramowania i udostępniane do nieodpłatnego pobrania przez użytkowników. Administratorzy systemów lub użytkownicy programów, w ramach swoich obowiązków sprawowania nadzoru nad bezpieczeństwem administrowanych systemów, sami powinni zatroszczyć się o pobranie odpowiednich łatek (np. ściągnąć z witryny internetowej producenta) i przeprowadzić wymagane aktualizacje systemu. Aktualizacje takie powinny być instalowane możliwie jak najszybciej. Toteż administratorzy systemów na bieżąco powinni śledzić komunikaty producentów użytkowanych systemów i monitorować inne źródła informacji poświęcone bezpieczeństwu oprogramowania, np. fora dyskusyjne, aby w porę podjąć stosowne działania.

5.9. *Dialery*

Dialer to wyspecjalizowany rodzaj programu komputerowego do łączenia się z Internetem przez inny numer dostępowy niż wybrany przez użytkownika. Programy te instalowane są w systemie użytkownika bez jego zgody i wiedzy. Celem działania *dialerów* nie jest wykradanie danych lub przejmowanie kontroli nad systemem, lecz wyłącznie przekierowywanie połączenia z Internetem poprzez inne (droższe) numery telefonu. *Dialery* zagrażają tylko użytkownikom komputerów, które z Internetem połączone są poprzez zwykłe modemy podłączone bezpośrednio do linii telefonicznej. W wyniku przekierowania połączenia z Internetem poprzez inny numer dostępowy, np. numer znajdujący się poza granicami kraju, operator nalicza dodatkowe impulsy, a użytkownik, zgodnie z podpisaną z operatorem umową, musi za te połączenia płacić wysokie rachunki telefoniczne. Zazwyczaj wykorzystywane w tych celach numery telefonów należą do operatorów mających siedzibę w odległych od Polski państwach, za połączenia z którymi są naliczane bardzo wysokie opłaty.

6. Technologie komputerowe, które mogą być wykorzystane do kradzieży danych

Złożoność systemów teleinformatycznych, ogromna ilość informacji zawartych w sieci oraz ciągle rosnąca liczba zagrożeń związanych z wykorzystywaniem Internetu skłaniają producentów oprogramowania do tworzenia wyspecjalizowanych narzędzi wykorzystywanych do wyszukiwania określonego rodzaju informacji, zarządzania określonymi zasobami w sieci, a nawet narzędzi umożliwiających rejestrację aktywności poszczególnych użytkowników. Stosowanie przez administratorów takich rozwiązań technologicznych jest często uzasadniane koniecznością optymalizacji kosztów administrowania oraz przede wszystkim potrzebami prowadzenia ciągłego monitoringu dla zapewnienia bezpieczeństwa administrowanej sieci.

Większość narzędzi tworzonych i stosowanych w wymienionych wyżej celach może być wykorzystywana również dla prowadzenie działań nielegalnych lub wręcz przestępczych. Jeśli narzędzia takie znajdą się w rękach niewłaściwych osób, mogą być wykorzystane np. do śledzenia działalności pracowników czy też ogólnie użytkowników monitorowanej sieci. Ze względu na swoje możliwości mogą być użyte nie tylko do oceny czasu, jaki pracownik spędza przy komputerze, wykonując swoje służbowe zadania, ale również do śledzenia jego prywatnej korespondencji i innych działań niezwiązanych z wykonywaniem powierzonych zadań, takich jak przeglądanie stron internetowych, korzystanie z komunikatorów czy udział w grach internetowych. Narzędzia takie można podzielić na lokalne, przeznaczone do stosowania przez administratora danej sieci, lub globalne, m.in. takie jak pliki *cookies* stosowane przez administratorów serwerów www w sieci Internet.

6.1. Pliki *cookies*

Cookies, czyli „ciasteczka", to niewielkie pliki tekstowe wysyłane przez serwer www i przechowywane lokalnie na komputerze użytkownika przeglądającego strony internetowe. Właściwością plików *cookies* jest to, że informacje zawarte w takim pliku może odczytać jedynie serwer, który je utworzył. Mechanizmy generowania plików *cookies* są stosowane najczęściej w rozbudowanych serwisach internetowych, w tym również w serwisach sklepów internetowych, stron wymagających logowania, stron reklamowych czy też stron służących do przeprowadzania różnego rodzaju sondaży wśród użytkowników Internetu. W tych ostatnich zastosowaniach pliki *cookies* wykorzystywane są m.in. do przeciwdziałania akcjom mającym na celu fałszowanie wyników sondaży poprzez wielokrotne głosowanie tych samych osób. W plikach *cookies* mogą być zapisane bardzo różnorodne informacje, m.in. niepowtarzalny identyfikator konta danego użytkownika w serwisie, dane stacji komputerowej, z której korzysta itp. Informacje zapisywane w tych plikach przez serwery www mogą być wykorzysty-

wane przez ich administratorów m.in. do monitorowania aktywności użytkowników odwiedzających jego serwisy.

Pliki *cookies* mogą być zapisywane w zasobach komputera użytkownika na trwale lub tymczasowo. Jeżeli w poleceniu utworzenia pliku nie zostanie określony czas jego istnienia, to plik taki zostanie usunięty po zakończeniu sesji, np. zamknięciu przeglądarki. Pliki bez określonego czasu ich istnienia nazywane są ciasteczkami sesyjnymi.

Gdy w plikach *cookies* zapisywany jest niepowtarzalny identyfikator użytkownika, może on należeć do kategorii danych, na podstawie których możliwe będzie zidentyfikowanie osoby, której on dotyczy. Wykorzystanie trwałych plików cookies lub podobnych rozwiązań zawierających niepowtarzalny identyfikator użytkownika pozwala na śledzenie użytkownika określonego komputera nawet w przypadku, gdy korzysta on z dynamicznie przedzielanych adresów IP. Gromadzenie danych na temat zachowań zidentyfikowanej w ten sposób osoby pozwalają na jeszcze większą możliwość skoncentrowania się na jej cechach. Pozostaje to w zgodzie z podstawową logiką dominującego modelu biznesowego, którego celem jest jak najlepsze poznanie użytkowników i w konsekwencji precyzyjne dobieranie przeznaczonych dla nich informacji reklamowych. Działania takie nie mogą być jednak wykonywane bez wiedzy osób, których dotyczą. Wymagają uzyskania ich uprzedniej zgody.

Trwałe pliki *cookies*, które zawierają niepowtarzalny identyfikator użytkownika komputera, mogą należeć do kategorii danych, na podstawie których można ustalić tożsamość osób i w tym rozumieniu mogą stanowić dane osobowe. Dlatego podlegają one ochronie wynikającej z przepisów ustawy o ochronie danych osobowych.

6.2. Technologia DPI (Głęboka Inspekcja Pakietów)

Technologia *Deep Packet Inspection* (DPI) to jedno z największych zagrożeń dla prywatności użytkowników sieci Internet. Polega ona na takiej analizie danych przesyłanych od nadawcy do

odbiorcy, która wykracza poza potrzeby technologiczne niezbędne do prawidłowego dostarczenia nadanej informacji. W analizie tej sięga się nie tylko do nagłówków wiadomości, które wskazują adresatów i są potrzebne do wykonania transmisji, ale także do treści przesyłanych informacji, aby wykorzystać je np. do akcji marketingowej[21]. W 2008 r. problemem wpływu skutków stosowania tej technologii na ochronę prywatności zainteresował się Komisarz Ochrony Danych Osobowych Kanady, inicjując publiczną dyskusję na ten temat, do której zaprosił przedstawicieli środowiska nauki oraz specjalistów z dziedziny telekomunikacji, prawa i informatyki[22]. Sprawą zajął się również Amerykański Kongres, po tym, jak w sieci pojawiły się informacje o kontrowersyjnych praktykach firmy NebuAd[23]. Zaniepokojeni tym zjawiskiem członkowie Komitetu Energii i Handlu Kongresu 1 sierpnia 2008 r. do AOL-u, Microsoftu, Google'a, Yahoo! i kilku innych firm wysłali listy z prośbą o zajęcie stanowiska wobec tej technologii.

W odpowiedzi firma Google[24] stwierdziła, że nie wykorzystuje technologii inspekcji pakietów jako narzędzia do analizowania zwyczajów internautów. Wskazała jednocześnie, że polityka prywatności korporacji „bazuje na trzech filarach: przejrzystości, możliwości wyboru i bezpieczeństwie". Spółka przypomniała również, że brała czynny udział w zainicjowanym przez Federalną Komisję Handlu projekcie stworzenia zestawu zasad dla branży reklamowej w Internecie i że zasad tych przestrzega. Google wyjaśniła, że dostarczane przez nią reklamy są

[21] http://www.getadvanced.net/learning/whitepapers/networkmanagement/Deep%20Packet%20Inspection_Whi te_Paper.pdf; Allot Communications, Digging Deeper into Deep Packet Inspection 1 (2007), ("DPI is the foremost technology for identifying . . . applications").

[22] http://dpi.priv.gc.ca/index.php/about/; Office of the Privacy Commissioner of Canada; About this proiect.

[23] http://www.fair.org/blog/tag/nebuad/; Posts Tagged 'NebuAd'; A New Challenge to Net Neutrality.

[24] http://209.85.203.104/external_content/services.google.com/blog_resources/google_policy_davidson_letter.pdf; Google responses to questions from the House Energy & Commerce Committee.

kontekstowe, a zatem dopasowane do gustów użytkownika. W celu wyznaczenia gustów brane są pod uwagę jedynie wpisane do wyszukiwarki słowa kluczowe lub tematyka witryn partnerskich, na których wyświetlane są boksy w obrębie jednej sesji.

6.3. Standardowy język baz danych i wstrzykiwanie jego kodu do stron WWW (SQL *injection*)

Większość obecnych stron informacyjnych i aplikacji internetowych wykorzystuje języki programowania oraz bazy danych do generowania tzw. dynamicznych stron informacyjnych. Podstawowym językiem komunikacji takiego systemu z informacjami zapisanymi w bazie danych jest język SQL. Jego funkcje stosuje się w praktyce do zarządzania i wyszukiwania informacji w bazach danych, na których oparte są serwisy internetowe. Wszelkie operacje na bazach w tym aspekcie sprowadzają się głównie do tego, aby treści zawarte w bazie serwisu zaprezentować w odpowiedni sposób na stronie internetowej. Prezentacja treści w takim przypadku może nastąpić poprzez wyświetlenie dynamicznie wygenerowanej strony internetowej lub poprzez zestawienie danych w wygenerowanym raporcie i wyświetlenie tego raportu w postaci strony internetowej. Jednak prezentacja to tylko jedna z funkcjonalności, która decyduje o sile serwisów opartych na takich rozwiązaniach. Możliwość wpisu i edycji treści przez ich użytkowników sprawia, że stają się oni jego współtwórcami. W celu powiązania użytkowników z ich działaniami oraz zgromadzonymi przez niego zasobami w serwisach internetowych, mechanizmów baz danych używa się również do obsługi procesu uwierzytelniania się użytkowników, a następnie ustanawiania relacji pomiędzy ich identyfikatorami i działaniami, które wykonają w danym serwisie.

Mimo niezaprzeczalnych korzyści i ogromnych możliwości, jakie niesie ze sobą technologia baz danych oparta o język zapytań SQL, trzeba mieć na uwadze, że jej funkcjonalność może zostać wykorzystana również w złych zamiarach. Użytkownik, który zna język zapytań SQL oraz zasady działania serwisów internetowych, może poszukiwać

luk i błędów, które pozostawili administratorzy i programiści serwisu. Umiejętnie dobrany ciąg znaków wprowadzony przez niego na przykład do formularza logowania lub wymuszenie wyszukiwania i wyświetlania w serwisie informacji, które nie są jawnie w nim wyświetlane, stanowią sposób na potencjalny atak. Powyższy ciąg znaków przekazywany w danych wejściowych modyfikuje zapytania przewidziane przez programistów tak, aby przekazać w nich dodatkowe parametry, co powoduje w konsekwencji umożliwienie nieautoryzowanego dostępu do kont użytkowników danego serwisu, a w skrajnych przypadkach do przejęcia uprawnień pozwalających na administrowanie danym systemem lub całym serwerem.

7. Stosowanie socjotechniki w atakach na bezpieczeństwo informacji w sieci

W celu skutecznego zapewnienia bezpieczeństwa informacji przesyłanych między nadawcą i odbiorcą w sieciach teleinformatycznych stosuje się skomplikowane algorytmy kryptograficzne oraz mechanizmy kontroli dostępu w dużej mierze bazujące na systemach uwierzytelniania wykorzystujących jedynie identyfikator i hasło użytkownika. Zarówno algorytmy kryptograficzne, jak i kontrola dostępu oparta na identyfikatorze i haśle użytkownika, w przypadku zapewnienia odpowiedniej złożoności hasła można uznać za wystarczająco bezpieczne.

Problem dotyczący skuteczności tych mechanizmów tkwi jednak nie tylko w ich jakości, ale również praktyce stosowania przez użytkowników. Często zdarzają się sytuacje, w których do utraty poufności dochodzi nie z powodu „złamania" zabezpieczeń, ale z powodu nieświadomego ich ujawnienia przez użytkowników. Metody stosowane do wyłudzania takich informacji od użytkowników nazywane są socjotechniką. Polegają one na wykorzystaniu wiedzy z dziedziny psychologii oraz podstawowych danych personalnych osób zatrudnionych w miejscu będącym obiektem ataku. Zainteresowany zdobyciem nieuprawnionych informacji telefonuje do osoby będącej

w posiadaniu potrzebnej informacji i podając się za pracownika technicznego firmy lub przełożonego ofiary, żąda natychmiastowego jej podania, argumentując to pilnymi potrzebami. Zaskoczony pracownik, przebywający np. na urlopie w danym dniu, nie odmawia „swojemu przełożonemu" i przekazuje poufne informacje. Innym przykładem socjotechniki jest wiadomość e-mail podszywająca się pod oficjalny komunikat, np. „Prosimy o przesłanie numeru swojej karty kredytowej w celu (...). Podpisano: z-ca ds. technicznych Banku" itp.

Jak stwierdził jeden z najbardziej znanych socjotechników, Kevin Mitnick, socjotechnika polega na „łamaniu" ludzi, a nie haseł.

7.1. *Phishing*

Phishing jest jednym z popularniejszych w ostatnim okresie sposobów kradzieży danych, w którym stosowane są elementy socjotechniki – metoda ta polega na przesłaniu do użytkownika konta wiadomości e-mail z prośbą o zalogowanie się na określoną stronę i uaktualnienie swoich danych czy np. zmianę hasła. Przestępcy wykorzystują nieświadomość adresata, który dokonuje aktualizacji swoich danych, i przekazuje im w ten sposób wszelkie informacje niezbędne do pełnego zarządzania kontem. Cechami charakterystycznymi dla tego rodzaju wiadomości są:

- masowe ich przesyłanie pocztą elektroniczną lub za pośrednictwem komunikatorów internetowych,
- zachęcanie użytkownika do kliknięcia linku przekierowującego na określoną witrynę, na której musi wprowadzić poufne dane, aby np. dokonać ich potwierdzenia lub ponownie aktywować konto,
- alarmowy charakter takich wiadomości, ostrzegający przed atakiem (w wiadomości często zawarta jest informacja, że ze względów bezpieczeństwa użytkownicy powinni odwiedzić witrynę www i potwier-

dzić swoje dane: nazwę użytkownika, hasło, numer karty kredytowej, numer PIN, numer PESEL itp.).

Cechą charakterystyczną *phisingu* jest to, że po kliknięciu linku przekierowującego na określoną witrynę otwiera się strona do złudzenia przypominająca wyglądem tę witrynę, na którą zamierzaliśmy się dostać.

Innym przykładem *phishingu* może być wiadomość e-mail rozsyłana z załącznikiem zawierającym złośliwe oprogramowanie służące przejęciu danych. Oprogramowanie to, w celu „uśpienia czujności odbiorcy", może być zawarte w załączniku pod nazwą np. kartka z życzeniami. Przestępcy, preparując takie wiadomości, stosują metody socjotechniki, które w maksymalnym stopniu mają wzbudzić zaufanie u odbiorcy. Wykorzystują w tym celu przyjęte w danym środowisku zwyczaje np. wysyłanie kartek do znajomych (kartki walentynkowe, z okazji Dnia Kobiet, świąt kościelnych, urodzin, imienin itp.). Dla zwiększenia zaufania przestępcy coraz częściej posługują się informacjami pozyskanymi z portali społecznościowych, na których użytkownicy sami dobrowolnie informują swoich znajomych, a przy okazji inne osoby, o imionach, dniach urodzin itp. Jak wynika z badań przeprowadzonych w 2007 r. na uniwersytecie Indiana[25], skuteczność *phishingu* przy użyciu spamu wykorzystującego informacje o grupach znajomych z portali społecznościowych wzrosła z 15% – kiedy danych tych nie wykorzystywano, do 72% – w przypadku, gdy je wykorzystano.

7.2. *Pfarming*

Pharming jest specyficzną odmianą *phishingu*. Polega on na modyfikowaniu zawartości serwera nazw domenowych DNS (*Domain Name Server*) w celu przekierowania użytkownika na sfałszowaną stronę, mimo prawidłowego wpisania adresu strony, którą rzeczywiście zamierzał on odwiedzić. Przekierowanie takie następuje na skutek zmiany ustawień protokołu TCP/IP lub modyfikację pliku lmhosts, który peł-

[25] http://indiana.edu~phishing/social-network-experiment/phishing-preprint.pdf; T. Jagatic, N. Johnson, M. Jacobson, F. Menczer. Social Phishing, ACM, October 2007

ni w komputerze użytkownika rolę lokalnego bufora nazw serwerów. Użytkownik, otwierając żądaną stronę, może nie być świadomy, że jest to inna strona niż ta, za pośrednictwem której zamierzał wykonać określone operacje. Wykonując zaś na tej stronie próbę logowania, wprowadza dane, które przechwytywane są przez przestępców. Jeżeli użytkownik korzysta z serwera proxy, atak taki może zostać przeprowadzony podczas określania nazwy DNS serwera. W wyniku ataku wszyscy użytkownicy korzystający z danego proxy zostaną przekierowani na fałszywy serwer.

7.3. Jak zapobiegać *phishingowi* i innym atakom socjotechnicznym

Jeśli dostaniemy konto wraz z hasłem do systemu, to jest ono jedynie naszą własnością i niedopuszczalne jest podawanie go przez telefon komukolwiek, nawet samemu administratorowi czy szefowi. W przypadku prośby administratora lub innej osoby o hasło do systemu w celu wykonania w naszej obecności odpowiednich testów lub innych działań (oczywiście, jeśli zaistnieje wyraźny powód), możemy to uczynić, ale bez zdradzania jego treści, tj. np. poprzez samodzielne jego wprowadzenie do systemu.

W praktyce działań przestępców komputerowych istnieje jednak wiele metod działania, w których bazując na zdobytych informacjach z zakresu zarządzania danym systemem czy też panujących przyzwyczajeniach użytkowników i typowych ich reakcjach, próbuje się, często z powodzeniem, uzyskać od nich informacje, które nie powinny być przez nich nigdy zdradzane. Metody te nazywane są powszechnie socjotechniką lub inżynierią socjalną (ang. *Social Engineering*).

Jak twierdzą specjaliści, podatność na metody inżynierii socjalnej zagraża każdemu użytkownikowi Internetu, bez względu na fakt, czy jest to użytkownik zaawansowany, czy początkujący. Żeby ustrzec się po części przed tego typu zagrożeniami, należy przede wszystkim mieć świadomość ich istnienia i zachować szczególną ostrożność. Najlepszymi sposobami ochrony są w tym przypadku nieobdarzanie nowo poznanych w sieci ludzi zaufaniem, jak również weryfikowanie wszelkich poleceń, zwłaszcza wydawanych telefonicznie lub pocztą elektroniczną pod ką-

tem tego, czy rzeczywiście pochodzą od osób, za które się one podają. W sieci na forach dyskusyjnych pojawiają się np. internauci, którzy bardzo chętnie deklarują pomoc w różnych kłopotach związanych z posługiwaniem się danym systemem i starają się pomagać poprzez chwilowe zalogowanie się do komputera użytkownika potrzebującego pomocy w celu rozwiązania problemu. Użytkownik musi mieś w takich sytuacjach świadomość, że chęć pomocy deklarowana przez nieznaną osobę niejednokrotnie może być podstępem prowadzącym do uzyskania zdalnego dostępu do jego komputera w celach przestępczych. Dlatego musi on mieć świadomość, że nawet jeśli używa wartych miliony dolarów systemów zabezpieczeń, to na nic się one nie zdadzą, jeśli sam umożliwia dostęp do swoich urządzeń potencjalnym przestępcom.

Użytkownik sieci szczególną uwagę powinien zatem zwracać na istniejące właściwości i funkcjonalność systemów, z których zamierza korzystać. Tak np. w przypadku korzystania z przeglądarek do wprowadzania poufnych informacji do formularzy internetowych, należy zwracać uwagę, czy ma ona wyłączoną opcję zapamiętywania danych. Pozostawienie tej opcji włączonej powoduje zapamiętywanie wprowadzanych danych na dysku lokalnego komputera. Ta sama uwaga dotyczy funkcjonalności przeglądarek w zakresie oferowanych opcji zapamiętywania identyfikatora i hasła przy logowaniu się do aplikacji internetowych, np. aplikacji udostępniającej pocztę elektroniczną.

Duże zagrożenie dla bezpieczeństwa danych stwarza nieprzemyślane korzystanie z portali społecznościowych. W większości z nich możliwe jest zarejestrowanie się użytkownika bez udziału mechanizmów, które mogłyby zweryfikować jego tożsamość.

Zarejestrowani użytkownicy mogą prezentować w tzw. profilach dowolne informacje o sobie i swojej działalności, zamieszczać swoje opinie, zdjęcia, filmy. Dane te mogą być wykorzystane przez osoby przygotowujące ataki metodą inżynierii socjalnej do zdobycia zaufania danej osoby albo podszycia się pod osobę należącą do kręgu jej przyjaciół.

Podsumowując należy stwierdzić, że sieć nie jest bezpiecznym narzędziem do wymiany informacji o naszym życiu prywatnym, relacjach ze znajomymi, w tym danych osobowych. Dlatego korzystając

z sieci, należy mieć świadomość istniejących zagrożeń i odpowiednio im przeciwdziałać. O zagrożeniach tych, zgodnie z art. 6 pkt 1 ustawy z 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. nr 144, poz. 1204 z późn. zm.), dostawcy usług powinni informować swoich klientów. Ponadto wszelkiego rodzaju zakazy i nakazy postępowania użytkowników wskazane w zalecanej do stosowania polityce bezpieczeństwa powinny być odpowiednio wyjaśnione i uzasadnione. Z badań wynika bowiem, że jeśli wymagania wprowadzone w polityce bezpieczeństwa są odpowiednio wyjaśnione i uzasadnione, to rzadziej dochodzi do ich naruszania[26].

8. Ewolucja działań przestępczych skierowanych na bezpieczeństwo sieci

Pierwsze programy działające niekorzystnie lub wręcz destrukcyjnie na prace systemu komputerowego, niszczące często efekty pracy użytkowników, pojawiły się już w roku 1982. Były to tzw. wirusy komputerowe, które rozprzestrzeniały się głównie poprzez „przyklejanie się" do plików zawierających programy lub nośników służących do ich przenoszenia, którymi najczęściej były wówczas tzw. dyskietki. Działanie destrukcyjne tych programów typu niszczenie danych, złe działanie komputera czy kradzież danych nie zawsze było głównym ich celem. Niektóre wirusy powodowały wówczas jedynie nietypowe, w pewnych okolicznościach, zachowanie się komputera. Wyświetlały informacje na ekranie, np. grafiki, wydawały sygnały, np. odgłosy stukania itp. Z upływem czasu, w miarę ewolucji systemów komputerowych, w tym głównie rozwoju Internetu, zmieniały się również cele i metody działania wirusów. Ich twórcy stosowali coraz nowsze techniki ich rozprzestrzeniania, wykorzystując nowe możliwości, jakie pojawiły się wraz z rozwojem technologii Internetowych, w tym poczty elektronicznej, stron www, protokołów wymiany danych typu FTP, komunikatorów itp.

[26] Tomasz Pełch, Stosowanie zabezpieczeń danych w systemach korporacyjnych: dobra wola czy prawny obowiązek?, „Gazeta IT" nr 18, listopad 2003 r.

W początkowym okresie większość znanych wirusów i robaków wykorzystywało pojedyncze luki w oprogramowaniu, co ograniczało ich szkodliwe działanie tylko do niektórych typów serwerów działających na określonej platformie, np. Code Red wykorzystał błąd przepełnienia bufora w serwerach Microsoft IIS. Oprogramowanie to było rozprowadzane zazwyczaj wyłącznie przez autorów, a szybkość jego rozprzestrzeniania się była na ogół ograniczona z powodu wykorzystywania, tak jak wspomniano, jednej luki w konkretnym systemie.

Obecnie coraz częściej pojawia się oprogramowanie, które zawiera mechanizmy skanowania szerokiego zestawu luk w oprogramowaniu, możliwość ataku na różne serwery (DNS, WWW, pocztowe, FTP itd.), a także na różne rodzaje systemów operacyjnych. Kierunek takich działań był przewidywany przez ekspertów już w roku 2001[27]. Inne są również narzędzia oraz sposoby tworzenia złośliwego oprogramowania. Jego autorzy, a często ich zorganizowane grupy, szeroko korzystają z możliwości dzielenia się pomysłami, jakie stworzył rozwój Internetu. Na grupach dyskusyjnych wymieniają swoje pomysły, dyskutują o nowych koncepcjach, których realizacja prowadzi do powstawania kolejnych, coraz bardziej szkodliwych generacji wirusów, robaków, koni trojańskich itp. Ukierunkowanie wysiłków przy tworzeniu szkodliwego oprogramowania ewoluuje stosownie do zmian w technologii oprogramowania, zmian w technologii sprzętu komputerowego, a także zmian w celach, które mają być atakowane. Tak np. w latach 2000-2001 wysiłki twórców szkodliwego kodu koncentrowały się na rozwoju robaków (*worm*) oraz programów integrujących funkcje wirusów, robaków i koni trojańskich. Modyfikacje kodu robaków miały na celu lepsze ich ukrywanie w zainfekowanym systemie i zwiększenie szybkości ich rozprzestrzeniania się (np. dzięki wprowadzeniu mechanizmów zapobiegających wielokrotnemu skanowaniu tych samych komputerów).

Obecnie problem złośliwego oprogramowania nie dotyczy tylko serwerów i komputerów osobistych. Wraz z masowym wejściem na rynek

[27] E. Skoudis; Counter Hack: A Step-by-Step Guide to Computer Attacks and Effective Defenses; Prentice Hall Ptr (2001)

nowych, mobilnych narzędzi służących komunikowaniu się wytworzone zostało złośliwe oprogramowanie, które również z tych urządzeń wykrada poufne dane lub zakłóca ich pracę. W 2004 r. pojawiły się pierwsze robaki atakujących telefony komórkowe. Do rozprzestrzeniania się robaków po raz pierwszy wykorzystano również technologię Bluetooth.

Skutkiem tak dynamicznego wzrostu „jakości", jak również intensyfikacji dystrybucji oprogramowania złośliwego jest spadek poczucia bezpieczeństwa wśród użytkowników Internetu. Tak np. według raportu[28] firmy Trend Micro Inc. w okresie od sierpnia 2006 r. do lutego 2007 r. liczba Amerykanów, którzy uważali Internet za bezpieczny, spadła o 6%. W tym samym stopniu zmniejszyła się również liczba osób, które przewidywały, że w ciągu następnych sześciu miesięcy Internet stanie się bezpieczniejszy. Spadek zaufania do bezpieczeństwa w Internecie zbiegł się w czasie ze zmianą głównych kierunków działania przestępców komputerowych. Wyświetlanie haseł reklamowych czy politycznych, odtwarzanie plików video albo utrudnianie pracy użytkownikowi nie są już głównymi celami ich działań. Cele te koncentrują się coraz bardziej na wykradaniu poufnych danych, takich jak identyfikatory i hasła do kont bankowych, numery kart kredytowych, kody PIN itp., przy jednoczesnym ukryciu tych działań przed użytkownikiem. Według raportu firmy Kaspersky Lab[29, 30] – jednego z producentów oprogramowania antywirusowego – przełomowy w produkcji oprogramowania szkodliwego był rok 2007. Autorzy raportu stwierdzają, że w roku 2007 nastąpił „upadek" epidemii powstawania dużej liczby wirusów i robaków powielanych z udziałem usług poczty elektronicznej, które były tworzone i rozprzestrzeniane przez jedną lub dwie osoby, najczęściej ich autorów. Z badań przeprowadzonych przez Kaspersky Lab wynika, że w latach

[28] http://trendmicro.mediaroom.com/index.php?s=43&item=25; Second Trend Micro Internet Confidence and Safety Survey; Trend Micro News Releases.

[29] http://vs.kaspersky.pl/download/analizy/ksb_2008_ewolucja_malware.pdf; Aleksander Gostew, Oleg Zajcew, Siergiej Golowanow; Kaspersky Security Bulletin 2008 – Ewolucja szkodliwego oprogramowania.

[30] http://vs.kaspersky.pl/download/analizy/ksb_2008_statystyki.pdf; Aleksander Gostew; Kaspersky Security Bulletin 2008 – Statystyki.

2007–2008 nastąpił wyraźny „podział pracy" różnych grup zajmujących się tworzeniem i dystrybucją oprogramowania szkodliwego. Większość trojanów, robaków i wirusów wykrytych w roku 2008 została stworzona wyłącznie na sprzedaż. Ich producenci oferowali nawet usługi wsparcia technicznego i doradztwo dotyczące np. wskazówek, jak obejść ochronę antywirusową, gdyby ta zaczęła wykrywać określone pliki. Jednocześnie tworzone oprogramowanie złośliwe ukierunkowane zostało na kradzież informacji dotyczących głównie kont bankowych, kart kredytowych i gier online. Ponadto oprócz czarnego rynku oprogramowania powstał czarny rynek poufnych informacji. Według raportu firmy Symantec[31], od lipca 2007 r. do czerwca 2008 r. całkowita wartość kradzionych towarów i usług, które były oferowane w globalnej sieci wyniosła 276 milionów dolarów. Najbardziej popularnym towarem były oczywiście – jak łatwo się domyśleć – numery kart kredytowych (31% rynku). Sprzedawano je za kwoty od 0,10 do 25 dolarów za sztukę. Tymczasem średni limit skradzionej karty wynosił 4 tysiące USD. Drugą grupę towarów stanowiły informacje o kontach bankowych. Sprzedawano je za kwoty od 10 do 1000 dolarów. Średnie saldo „sprzedawanego" konta wynosiło 40 tysięcy USD, a całkowita wartość zdeponowanych środków 1,7 mld USD. Symantec prześledził łącznie 69 130 użytkowników, którzy opublikowali ponad 44 miliony ogłoszeń sprzedaży nielegalnych produktów.

Wspomniany podział zadań w tworzeniu, dystrybucji i wykorzystywaniu złośliwego oprogramowania sprawia, że walka z cyberprzestępczością jest coraz trudniejsza. Przeprowadzane ataki, w ocenie specjalistów z Kaspersky Lab, Panda Lab[32], Symantec[33], jak również z innych ośrodków, są coraz bardziej złożone, a także ukryte przed użyt-

[31] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_rep-ort_11-2008-14525717.en-us.pdf; Symantec Report on the Underground Economy July 07–June 08; Published November 2008.

[32] http://www.pandasecurity.com/img/enc/Quarterly_Report_PandaLabs_Q1_2009.pdf; Quarterly Report Panda-Lab (January-March 2009)

[33] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xi-v_04-2009.en-us.pdf; Symantec Global Internet Security Threat Report – Trends for 2008; Volume XIV, Pu-blished April 2009.

kownikiem. Potwierdzeniem tego zjawiska były dwa zmasowane ataki hakerów na strony internetowe przeprowadzone w okresie kwiecień – październik 2008 r. W pierwszym z nich, który miał miejsce w okresie kwiecień – czerwiec 2008 r., zaatakowane zostały prawie 2 miliony zasobów internetowych na całym świecie. Atak polegał na wstrzyknięciu do zaatakowanej strony kodu SQL[34] w celu osadzenia w niej poleceń, które przekierowywały użytkowników na strony przestępców, które infekowały komputery użytkowników szkodliwym oprogramowaniem szpiegowskim. W roku 2008 powróciły wirusy plikowe, które w porównaniu do tych z lat 80. poprzedniego stulecia, rozszerzone były w swoim działaniu o funkcje wykradania danych. Wirusy te mogą się rozprzestrzeniać za pośrednictwem wymiennych nośników danych, w tym popularnych dziś dysków i pamięci USB. Większość z nich to wirusy polimorficzne, czyli takie, których kod zmienia się w czasie, nie zmieniając oryginalnego algorytmu w nim zawartego. To stwarza dodatkowe trudności dla producentów rozwiązań antywirusowych w tworzeniu procedur ich wykrywania i „leczenia" w akceptowalnym przedziale czasu. Okazało się np., że robaki znajdujące się w pamięci USB potrafią obejść tradycyjną ochronę dla lokalnych sieci wewnętrznych instytucji (np. zabezpieczenie antywirusowe dla serwerów pocztowych, zapory sieciowe i rozwiązania antywirusowe dla wielu innych serwerów, m.in. serwerów baz danych, serwerów plików itp.). Po przedostaniu się do sieci wewnętrznej na skutek obejścia ochrony, robaki takie mogą szybko rozprzestrzeniać się w całej sieci, czyniąc ogromne szkody, takie jak utrata poufności przetwarzanych danych, ich zniszczenie lub uszkodzenie oraz wiele godzin pracy informatyków przy usuwaniu skutków ich działania.

8.1. Prognozy zagrożeń dla bezpieczeństwa sieci na rok 2009

Badania przeprowadzone w pierwszej połowie 2008 r. przez PandaLabs – laboratorium firmy Panda Security – wykazały, że ilość krążącego w sieci złośliwego oprogramowania wzrosła w tym okresie do niespotykanych dotąd rozmiarów. Liczba szkodliwych programów,

[34] Patrz punkt 6.3 – Standardowy język zapytań do baz danych (SQL *injection*).

które utrudniały życie internautom, tylko w okresie między styczniem a sierpniem 2008 r. była większa niż suma zagrożeń, które pojawiły się w Internecie na przestrzeni ostatnich 17 lat. Niepokojące jest również to, że według prognoz PandaLabs, rok 2009 może przynieść kolejny niechlubny cyberprzestępczy rekord. Specjaliści z PandaLabs przewidują, że trojany bankowe służące wykradaniu danych oraz fałszywe programy antywirusowe nadal należeć będą do najpopularniejszych rodzajów złośliwego oprogramowania. Do ich dystrybucji przewidywane jest coraz szersze wykorzystywanie portali społecznościowych. Będzie się to odbywało nie tylko poprzez rozpowszechnianie robaków wśród ich użytkowników, ale także poprzez wykorzystywanie złośliwych kodów do kradzieży poufnych danych. W badaniach tych przewiduje się dalszy wzrost liczby ataków polegających na wprowadzaniu kodu SQL (SQL *injection*) do stron www, które powodują następnie infekcję komputerów niczego nieświadomych użytkowników, gdy ci odwiedzają te zainfekowane witryny. Do przeprowadzania ataków na serwery www cyberprzestępcy wykorzystywać będą luki w zabezpieczeniach serwerów, na których znajdują się odwiedzane strony. PandaLabs przewiduje również, że w 2009 r. nastąpi wzrost zastosowań narzędzi służących do pakowania i ukrywania złośliwego oprogramowania, co zwiększy trudności ich wykrywania i usuwania. Cyberprzestępcy będą starali się unikać stosowania standardowych narzędzi dostępnych na forach czy witrynach internetowych na rzecz własnych produktów ukrywających kod złośliwego oprogramowania, aby uniknąć wykrycia przez systemy zabezpieczające na podstawie sygnatur[35]. Nie przewiduje się natomiast wirusów uniemożliwiających działanie systemu lub blokujących otwieranie plików, które były popularne 10 lat temu. Teraz przestępcom zależy głównie na zdobyciu danych przydatnych im do dalszych działań. Dlatego trzeba się przygotować na ukryte zagrożenia, które osadzone w systemie użytkownika, będą wykorzystywane

[35] Sygnatura wirusa – to specyficzny ciąg danych występujących w kodzie wirusa, który umożliwia jego szybką identyfikację. Sygnatury służą do wykrywania większości wirusów (oprócz polimorficznych) przez systemy antywirusowe.

do kradzieży informacji (hasła do gier, usług telekomunikacyjnych, informacji bankowych itp.). Laboratorium Panda Security prognozuje również gwałtowny wzrost ilości złośliwego oprogramowania wymierzonego w nowe platformy sprzętowe i programowe, takie jak Mac OS Leopard X, Linux czy iPhone. Nie będzie to jednak wzrost tak duży, jak w przypadku systemów Windows ze względu na mniejszą popularność tych platform i wynikającą z tego mniejszą skuteczność przeprowadzanych ataków.

Niepokojący raport (patrz przypis na stronie 57) na temat prognoz wzrostu zagrożeń przedstawiła również firma Symantec. Według jej danych, tylko w 2008 r. opracowanych zostało ponad 1,6 miliona nowych sygnatur dla wszelkiego typu złośliwego oprogramowania. Stanowi to aż 60% wszystkich sygnatur utworzonych do tej pory w laboratoriach tej firmy. Dane firmy Symantec wskazują również na dużą aktywność złośliwego oprogramowania w 2008 r. (w każdym miesiącu ubiegłego roku, na całym świecie systemy ochrony firmy Symantec odnotowywały około 245 milionów prób ataków). Przy czym głównym źródłem infekcji były serwery internetowe przechowujące strony www, a celem ataków – najczęściej kradzież poufnych danych (blisko 90% wszystkich ataków). Dane te aż w 76% przypadków wykradano poprzez użycie oprogramowania do zapisywania znaków wprowadzanych na klawiaturze (tzw. keyloggerów). W pozostałych przypadkach zaś, w wyniku innych ataków, głównie phishingu, którego wzrost w 2008 r. w stosunku do roku 2007 odnotowano na poziomie około 66%. Ma to silny związek ze wzrostem liczby niezamawianej korespondencji poczty elektronicznej. W 2008 r. jej liczba wzrosła o blisko 190% w porównaniu z rokiem 2007, osiągając w skali globalnej poziom około 349,6 miliarda. Korespondencja taka rozsyłana była przy użyciu zainfekowanych komputerów użytkowników (zombie), połączonych w coraz liczniejsze sieci, tzw. botnety. Według prognoz firmy Symantec, zaobserwowane w 2008 r. trendy wzrostu zagrożeń szkodliwym oprogramowaniem będą miały miejsce również w roku 2009. Nadal nasilać się będą zagrożenia kodem złośliwego

oprogramowania dystrybuowanym poprzez strony www, pocztę elektroniczną, komunikatory internetowe i sieci P2P[36].

Podobne prognozy w zakresie nasilania się liczby ataków oraz kierunków ewolucji złośliwego oprogramowania przedstawiły również laboratoria innych znanych firm zajmujących się wytwarzaniem oprogramowania zabezpieczającego przed złośliwym oprogramowaniem.

9. Obowiązki administratora danych

Systematyczny wzrost zagrożeń dla bezpieczeństwa informacji przetwarzanej przy użyciu systemów teleinformatycznych oraz prawne wymogi ochrony prywatności sprawiają, że zastosowanie nowoczesnych narzędzi, w tym usług telekomunikacyjnych do przetwarzania danych wymaga coraz bardziej profesjonalnego podejścia do zarządzania ich bezpieczeństwem. Podejmowane przez administratora danych działania mające na celu zbudowanie systemu zarządzania bezpieczeństwem powinny obejmować:

1) przeprowadzenie analiza ryzyka w zakresie utraty poufności przetwarzanych danych, ich zniszczenia, utraty lub nieuprawnionej modyfikacji,
2) ustanowianie – odpowiedniej do celów i zakresu przetwarzania danych – polityki bezpieczeństwa i procedur zarządzania tym bezpieczeństwem,
3) wdrożenie i stosowanie środków przewidzianych w ustanowionej polityce bezpieczeństwa,

[36] Sieci P2P – od ang. *peer-to-peer* – równy z równym, są sieciami, w których strony komunikacji posiadają równorzędne prawa (w przeciwieństwie do modelu klient-serwer). Sieci P2P wykorzystywane są przez internautów do wymiany różnych danych, np. muzyki, filmów, książek w wersji elektronicznej itp. Istnieje wiele modeli sieci P2P (np. Napster, Gnutella, FastTrack, eDonkey). Do zbudowania sieci P2P należy użyć specjalnego oprogramowania.

4) szkolenie pracowników w zakresie zgodnego z prawem przetwarzania danych osobowych, w tym odpowiedzialności za jego naruszenie,
5) zapewnienie odpowiednich relacji między administratorem danych i podmiotem, któremu powierzono przetwarzanie danych lub administratorem danych i użytkownikiem będącym jednocześnie podmiotem, którego dane są przetwarzane[37].

W tym ostatnim przypadku podmiotem, który przetwarza dane, może być zarówno wyspecjalizowana firma, której zlecamy wykonywanie określonych czynności przetwarzania danych w ramach tzw. umowy powierzenia przetwarzania, o której mowa w art. 31 ustawy, jak i osoba fizyczna, której dane dotyczą. W przypadku powierzenia przetwarzania danych innemu podmiotowi, administrator danych musi mieć świadomość, że nie zwalnia go to z odpowiedzialności za bezpieczeństwo i jakość tego przetwarzania. W trosce o właściwe wypełnienie swoich obowiązków, już w zawieranej umowie powierzenia administrator powinien zapewnić sobie prawo do wykonywania audytu i kontroli przetwarzania powierzonych danych. W umowie powinien zawrzeć również procedury postępowania z danymi na wypadek jej zerwania lub wygaśnięcia. W czasie trwania umowy administrator danych powinien sprawować rzeczywistą kontrolę nad procesem ich przetwarzania poprzez okresowe wykonywanie audytów w zakresie realizacji celów przetwarzania zgodnie z umową oraz w zakresie zgodności z warunkami określonymi w przepisach o ochronie danych osobowych, w tym właściwego ich zabezpieczenia. Oznacza to, że elementy zarządzania bezpieczeństwem, o których mowa wyżej w punktach od 1 do 4, powinny być przedmiotem kontroli podmiotu, któremu administrator powierzył przetwarzanie danych. Administrator danych kontrole takie powinien przeprowadzać w ramach realizacji ciążącego na nim obowiązku zapewnienia legalności przetwarzania zebranych danych oraz właściwego ich zabezpieczenia.

[37] Przypadek użytkownika systemu będącego osobą, której dane są przetwarzane, dotyczy głównie portali społecznościowych i innych podobnego typu aplikacji internetowych, w których użytkownik sam decyduje o wprowadzanych do systemu danych.

Inne relacje między administratorem danych a podmiotem, któremu powierzono przetwarzanie, występują w sytuacji, gdy tym ostatnim jest osoba fizyczna, której dane dotyczą. W przypadkach takich nie mamy do czynienia z umową powierzenia, o której mowa w art. 31 ustawy. W przypadkach, kiedy administrator danych stwarza użytkownikom Internetu możliwości wprowadzenia własnych danych do systemu i w pewnym zakresie również możliwości ich przetwarzania, nie występuje typowa umowa powierzenia przetwarzania, o której mowa w art. 31 ustawy. Przykładem takich rozwiązań są sklepy internetowe, portale społecznościowe, systemy bankowości elektronicznej itp. Osoba, która sama zarejestrowała się w takim systemie, powinna mieć wyłącznie uprawnienia do edycji danych, które jej dotyczą. W odniesieniu do takich osób administrator systemu, w którym dane są przetwarzane, nie posiada takich możliwości kontrolnych, jak w odniesieniu do osób u niego zatrudnionych, które upoważnił do przetwarzania danych. Nie oznacza to jednak zmniejszenia odpowiedzialności administratora danych za zgodność przetwarzania z przepisami prawa.

W przypadku jednak, kiedy administrator danych przekazał użytkownikowi uprawnienia do zarządzania jego własnymi danymi, użytkownik ten staje się współodpowiedzialny za ich jakość i bezpieczeństwo[38]. Aby użytkownik mógł jednak w takim procesie uczestniczyć, powinien być przez administratora danych poinformowany o istniejących zagrożeniach bezpieczeństwa przetwarzania, jak również o środkach i procedurach bezpiecznego przetwarzania, jakie powinien stosować.

Administratorzy danych osobowych muszą mieć świadomość, że konkretnych procedur czy środków, jakie należy zastosować w celu zapewnienia odpowiedniej ochrony danych, nie znajdą wprost w przepisach ustawy o ochronie danych osobowych ani w rozporządzeniu ministra spraw wewnętrznych i administracji z 29 kwietnia 2004 r.

[38] Sytuacja, kiedy administrator danych osobowych przekazuje użytkownikowi uprawnienia do zarządzania jego własnymi danymi dotyczy większości systemów internetowych, w których osoby samodzielnie się rejestrują i wpisują swoje dane (portale społecznościowe, grupy dyskusyjne, komunikatory internetowe, darmowa poczta elektroniczna itp.).

w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. nr 100, poz. 1024), zwanym dalej rozporządzeniem, definiującym wymagane poziomy ochrony. Zarówno ustawa o ochronie danych osobowych, jak i rozporządzenie w zakresie dotyczącym bezpieczeństwa przetwarzania wskazują jedynie na warunki, jakie powinny być spełnione, a nie na sposób lub środki, przy użyciu których powinny być one osiągnięte. Wybór odpowiednich środków technicznych i organizacyjnych należy zatem do zadań administratora danych.

Należy zaznaczyć, że nie jest to zadanie łatwe. Administratorzy danych muszą mieć świadomość, że ogromne zasoby informacji zgromadzone w systemach informatycznych są intratnym kąskiem dla konkurencji oraz przestępców gospodarczych. Niepokojącym zjawiskiem jest to, że proceder ataków na systemy informatyczne instytucji, jak również stacje komputerowe użytkowników indywidualnych w celu kradzieży tożsamości elektronicznej ciągle narasta. Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji w raporcie GENERAL Report 2007, a także swojej stronie internetowej (http://www.enisa.europa.eu/) informuje, że działania cyberprzestępców mogą wkrótce poważnie zagrozić gospodarce UE. Przestrzega przy tym przed poważnymi zagrożeniami, jakimi są sieć około 6 mln zainfekowanych komputerów, które mogą służyć do przeprowadzenia ataku oraz ciągle zbyt niska świadomość zagrożeń wśród użytkowników Internetu.

Informacje powyższe oraz doniesienia prasowe z kraju i zagranicy o wyciekach danych osobowych czy np. nieprawidłowościach w systemach internetowych, dowodzą, że wszystkie elementy zarządzania bezpieczeństwem (wymienione na początku tej części w punktach od 1 do 5) należy traktować bardzo poważnie i z dużą odpowiedzialnością.

9.1. Analiza ryzyka

Ryzyko bezpieczeństwa informacji można zdefiniować jako prawdopodobieństwo wystąpienia zagrożenia i powstania szkód lub zniszczeń w zasobach systemu oraz przerw lub zakłóceń w jego prawidłowym funkcjonowaniu.

Głównym elementem procesu zarządzania ryzykiem bezpieczeństwa informacji jest analiza ryzyka, której celem jest identyfikacja zasobów systemu, odpowiadających im podatności i zagrożeń, a także oszacowanie prawdopodobieństwa ich wystąpienia oraz wielkości potencjalnych strat. Istnieją dwie podstawowe grupy metod przeprowadzania analizy ryzyka – kwantyfikatywne (ilościowe) oraz kwalifikatywne (jakościowe).

Metody kwantyfikatywne (ilościowe) opierają się na matematycznych obliczeniach wpływu zagrożenia na bezpieczeństwo systemu oraz prawdopodobieństwo jego wystąpienia. Operują wyłącznie na danych liczbowych zaczerpniętych z analizy danych statystycznych i historycznych. Najczęściej stosowane wartości w kwantyfikatywnych metodach analizy ryzyka to: wartość monetarna, wartość procentowa, liczba wystąpień i prawdopodobieństwo wystąpienia danego zdarzenia.

Metody kwalifikatywne (jakościowe) są znacznie bardziej subiektywne, gdyż bazują na wiedzy i ocenie ekspertów. Wykorzystuje się w nich miary opisowe, które mogą posiadać liczbowe odpowiedniki (1 – ryzyko małe, 4 – ryzyko maksymalne itd.).

Typowy proces szczegółowej analizy ryzyka bezpieczeństwa informacji oparty na metodzie kwalifikatywnej składa się z sześciu podstawowych etapów:

- identyfikacji i oceny zasobów,
- identyfikacji zagrożeń,
- identyfikacji istniejących zabezpieczeń,
- identyfikacji podatności,
- szacowania ryzyka,
- opracowania rekomendacji.

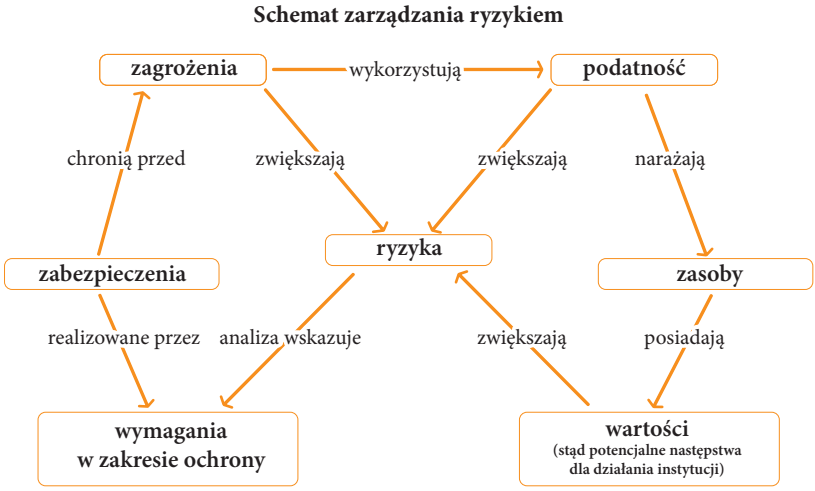
Analiza ryzyka powinna być wykonana przez każdą organizację wdrażającą system zarządzania bezpieczeństwem informacji i mieć na celu doprowadzenie do obniżenia ryzyka do takiego poziomu, w którym organizacja będzie zdolna ponieść ciężar strat spowodowanych przez kradzież lub modyfikację danych. Podstawowymi zadaniami analizy ryzyka jest zatem zidentyfikowanie, dla danego środowiska przetwarzania (środowisko informatyczne, zabezpieczenia fizyczne do obiektów, nośników danych, serwerów, stacji roboczych, mediów transmisyjnych itp.) naturalnych zagrożeń i oszacowanie potencjalnych skutków ich wystąpienia, a następnie wyszukanie i zaproponowanie środków redukujących prawdopodobieństwo i/lub skutki ich wystąpienia. Proces taki, jak już wspomniano wyżej, może przebiegać według różnych schematów.

Można np. skorzystać ze schematów wskazanych w polskich normach technicznych dotyczących zarządzania ryzykiem, na jakie narażone jest bezpieczeństwo systemów informatycznych. Do norm tych należą m.in. normy: PN-I-13335-1, PN-ISO/IEC 17799 oraz PN-ISO/IEC 27001.

Według np. normy PN-I-13335-1, zarządzanie ryzykiem jest jednym z kilku elementów procesu zarządzania bezpieczeństwem systemów teleinformatycznych, których celem jest udzielenie odpowiedzi na następujące pytania:

- **co złego może się wydarzyć?**
- **jakie jest prawdopodobieństwo, że wydarzy się coś złego?**
- **jakie skutki dla systemu informatycznego i organizacji będą miały te wydarzenia?**
- **jak i o ile możemy zmniejszyć straty?**

Norma PN-I-13335-1 wskazuje na związki, jakie występują między poszczególnymi elementami w procesie zarządzania ryzykiem (zostały one przedstawione na Rys. 1)



Rys. 1. Zależności występujące między poszczególnymi elementami systemu zarządzania ryzykiem przy ocenie ryzyka według normy PN-I-13335-1.

Należy pamiętać, że ryzyko możemy zmniejszać, ale nigdy całkowicie go nie wyeliminujemy. Ryzyko, które pozostanie w naszym systemie, mimo zastosowania fizycznych, organizacyjnych i technicznych środków ochrony, nazywamy ryzykiem szczątkowym. W zarządzaniu ryzykiem istotna jest odpowiedź na pytanie, do jakiego poziomu warto je obniżać. Okazuje się, że na pewnym poziomie dodawanie nowych zabezpieczeń jest znacznie kosztowniejsze niż wzrost wartości bezpieczeństwa, które przy ich pomocy można osiągnąć.

Uniwersalna zasada mówi, że ryzyko należy obniżać do poziomu, w którym organizacja będzie zdolna ponieść ciężar strat spowodowanych przez zrealizowane zagrożenia i kontynuować swoją działalność. Ryzyko szczątkowe tego typu nazywamy ryzykiem akceptowalnym.

9.2. Polityka bezpieczeństwa

Zgodnie z § 3 i § 4 rozporządzenia ministra spraw wewnętrznych i administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, administrator danych obowiązany jest do opracowania w formie pisemnej i wdrożenia polityki bezpieczeństwa. Pojęcie „polityka bezpieczeństwa" użyte w rozporządzeniu należy rozumieć jako zestaw praw, reguł i praktycznych doświadczeń dotyczących sposobu zarządzania, ochrony i dystrybucji danych osobowych wewnątrz określonej organizacji. Trzeba zaznaczyć, że zgodnie z art. 36 ust. 2 oraz art. 39a ustawy o ochronie danych osobowych, polityka bezpieczeństwa, o której mowa w rozporządzeniu, powinna odnosić się całościowo do problemu zabezpieczenia danych osobowych przetwarzanych przez administratora danych, tj. zarówno do zabezpieczenia danych przetwarzanych tradycyjnie, jak i danych przetwarzanych w systemach informatycznych. Celem polityki bezpieczeństwa jest wskazanie działań, jakie należy wykonać, oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby właściwie zabezpieczyć dane osobowe.

Polska Norma PN-ISO/IEC 17799:2005, określająca praktyczne zasady zarządzania bezpieczeństwem informacji w obszarze technik informatycznych, jako cel polityki bezpieczeństwa wskazuje „zapewnienie kierunków działania i wsparcie kierownictwa dla bezpieczeństwa informacji". Zaznacza się, że dokument polityki bezpieczeństwa powinien deklarować zaangażowanie kierownictwa i wyznaczać podejście instytucji do zarządzania bezpieczeństwem informacji. Jako minimum wskazuje ona wiele elementów, jakie dokument określający politykę bezpieczeństwa powinien zawierać. Wykaz tych elementów zestawiony został w niżej zamieszczonej ramce.

Dokument określający politykę bezpieczeństwa powinien zawierać:

a) określenie mechanizmów umożliwiających współużytkowanie informacji (mechanizmów dostępu do danych i specyfikacji zakresu uprawnień do ich przetwarzania);

b) oświadczenie o intencjach kierownictwa, potwierdzające cele i zasady bezpieczeństwa informacji w odniesieniu do strategii i wymagań biznesowych;

c) strukturę wyznaczania celów stosowania zabezpieczeń, w tym strukturę szacowania i zarządzania ryzykiem;

d) krótkie wyjaśnienie polityki bezpieczeństwa, zasad, norm i wymagań zgodności mających szczególne znaczenie dla organizacji, zawierające:

1) zgodność z prawem, regulacjami wewnętrznymi i wymaganiami wynikającymi z umów;

2) wymagania dotyczące kształcenia, szkoleń i uświadamiania w dziedzinie bezpieczeństwa;

3) zarządzanie ciągłością działania biznesowego;

4) konsekwencje naruszenia polityki bezpieczeństwa;

e) definicje ogólnych i szczególnych obowiązków w odniesieniu do zarządzania bezpieczeństwem informacji, w tym zgłaszania incydentów związanych z bezpieczeństwem informacji;

f) odsyłacze do dokumentacji mogącej uzupełniać politykę, np. bardziej szczegółowych polityk bezpieczeństwa i procedur dotyczących poszczególnych systemów informatycznych lub zalecanych do przestrzegania przez użytkowników zasad bezpieczeństwa.

Wykaz elementów stanowiących politykę bezpieczeństwa według PN-ISO/IEC 17799:2005.

Wymienione wyżej zalecenia można w pełni stosować do dokumentacji polityki bezpieczeństwa, o której mowa w § 4 rozporządzenia. Warto podkreślić, że dokument określający politykę bezpieczeństwa nie powinien mieć charakteru zbyt abstrakcyjnego. Zasady postępowania określone w polityce bezpieczeństwa powinny zawierać uzasadnienie wyjaśniające przyjęte standardy i wymagania. Wyjaśnienia i uzasadnienia dotyczące zalecanych metod sprawiają na ogół, że rzadziej dochodzi do ich naruszenia.

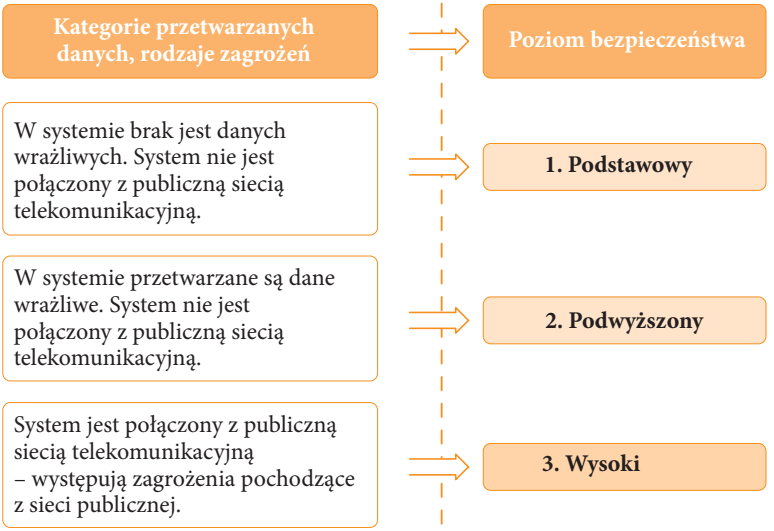
Dokument, o którym mowa w § 4 rozporządzenia, w zakresie merytorycznym powinien koncentrować się na wprowadzeniu i stosowaniu środków bezpieczeństwa przetwarzania danych osobowych, co wynika z art. 36 ustawy. Prawidłowe zarządzanie zasobami, w tym również zasobami informacyjnymi, zwłaszcza w aspekcie bezpieczeństwa informacji, wymaga właściwej identyfikacji tych zasobów oraz określenia miejsca i sposobu ich przechowywania. Wybór odpowiednich dla poszczególnych zasobów metod zarządzania ich ochroną i dystrybucją zależny jest zaś od zastosowanych nośników informacji, rodzaju używanych urządzeń, sprzętu komputerowego i oprogramowania. Dlatego w § 4 rozporządzenia ustawodawca wskazał, że:

Polityka bezpieczeństwa powinna zawierać w szczególności:

1) **wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;**
2) **wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;**
3) **opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;**
4) **sposób przepływu danych pomiędzy poszczególnymi systemami;**
5) **określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przy przetwarzaniu danych.**

Duża część polityki bezpieczeństwa, o której mowa w § 4 rozporządzenia, poświęcona jest szczegółowej inwentaryzacji posiadanych zasobów i ich charakterystyce. Ta część, opisująca faktyczny stan posiadanych zasobów informacyjnych, w tym ewentualne przepływy danych między różnymi systemami informatycznymi i/lub bazami danych, ma szczególne znaczenie dla oceny ryzyka, na jakie przetwarzane dane są narażone, i wyboru odpowiednich środków bezpieczeństwa. Natomiast informacje zawarte w punkcie 5 polityki bezpieczeństwa powinny stanowić opis środków technicznych i organizacyjnych, jakie zostały zastosowane przez administratora danych w celu zapewnienia przetwarzanym danym odpowiedniej ochrony. Środki te powinny być takie, aby zidentyfikowane ryzyko zostało zredukowane do akceptowalnego poziomu. Wybór konkretnych środków zarówno technicznych, jak i organizacyjnych pozostawia się do decyzji administratora danych. Podejmując w powyższym zakresie decyzję, administrator danych, niezależnie od wyników przeprowadzonej analizy ryzyka, zobowiązany jest do zastosowania co najmniej takich środków bezpieczeństwa, jakie zostały wskazane w rozporządzeniu.

Minimalne środki bezpieczeństwa wskazane w rozporządzeniu zależne są od rodzaju zagrożeń oraz kategorii przetwarzanych danych. Rozporządzenie wprowadza w tym celu 3 poziomy zabezpieczeń – podstawowy, podwyższony i wysoki, których charakterystykę prezentuje Rysunek 2.



Rys. 2. Poziomy bezpieczeństwa według przepisów rozporządzenia ministra spraw wewnętrznych i administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

9.3. System zarządzania bezpieczeństwem

System zarządzania bezpieczeństwem zaprojektowany przez administratora danych musi być spójny i obejmować wszystkie obszary przetwarzania danych. Należy bowiem pamiętać o wspomnianych już specyficznych właściwościach systemów zabezpieczeń mówiących o tym, że *żeby bowiem skutecznie zabezpieczyć system należy usunąć „wszystkie" jego słabości i podatności na znane rodzaje ataków, jak również ataki, które mogą pojawić się w najbliższej przyszłości, zaś aby skutecznie zaatakować – wystarczy znaleźć jedną słabość danego systemu i stosownie ją wykorzystać*. Właściwość ta ma szczególne znaczenie w przypadku odnoszącym się do bezpieczeństwa systemu, który połączony jest z siecią publiczną. W celu zbudowania właściwych zabezpieczeń

dla takiego systemu, a następnie odpowiednich procedur zarządzania zastosowanymi środkami zabezpieczajacymi, warto posiłkować się istniejącymi metodykami, takimi jak normy PN-ISO/IEC 17799:2005 czy PN-ISO/IEC 27001:2007. Wymienione dokumenty normalizacyjne dotyczą bezpośrednio sposobu budowy systemu zabezpieczeń, a także zarządzania bezpieczeństwem informacji. Dokument PN-ISO/IEC 17799:2005, którego pełna nazwa brzmi „PN-ISO/IEC 17799:2005 *Technika informatyczna. Praktyczne zasady zarządzania bezpieczeństwem informacji*" w kilkunastu rozdziałach opisuje elementy, na które administrator danych powinien zwrócić uwagę, projektując system zabezpieczenia danych. Spośród nich na szczególną uwagę zasługują rozdziały 10, 11 i 12, które opisują odpowiednio: zarządzanie systemami i sieciami, kontrolę dostępu oraz pozyskiwanie, rozwój i utrzymanie systemów informacyjnych.

Zarządzanie systemami i sieciami

W rozdziale tym omawiane są m.in. takie elementy mające bezpośredni wpływ na bezpieczeństwo systemu połączonego z siecią publiczną, jak:

- zarządzanie bezpieczeństwem sieci (zabezpieczenia sieciowe, bezpieczeństwo usług sieciowych),
- wymiana informacji (polityka i procedury wymiany informacji, umowy dotyczące wymiany informacji, transportowanie nośników fizycznych, postępowanie z wiadomościami elektronicznymi, procedury administrowania biznesowymi systemami informacyjnymi),
- usługi handlu elektronicznego (bezpieczeństwo transakcji on-line, udostępnianie informacji publicznie dostępnej).

Kontrola dostępu

W rozdziale tym omawianych jest wiele zagadnień związanych z kontrolą dostępu do danych, takich jak:

- wymagania biznesowe dla kontroli dostępu,
- zarządzanie dostępem użytkowników,
- odpowiedzialność użytkowników,
- kontrola dostępu do sieci,
- kontrola dostępu do systemów operacyjnych,
- kontrola dostępu do aplikacji i informacji,
- przetwarzanie mobilne i praca na odległość.

Wiele z wymienionych w tym rozdziale zagadnień ma szczególne znaczenie dla budowy systemu zabezpieczeń w środowisku sieciowym. Do najważniejszych należą:
Kontrola dostępu do sieci. W obszarze tym norma zwraca uwagę na takie elementy, jak: polityka dotycząca korzystania z usług sieciowych, uwierzytelnianie użytkowników przy połączeniach zewnętrznych, identyfikacja urządzeń w sieciach, ochrona zdalnych portów diagnostycznych i konfiguracyjnych, rozdzielanie sieci, kontrola połączeń sieciowych, zabezpieczenie *routingu* w sieciach).
Kontrola dostępu do systemów operacyjnych. W kwestii tej dokument zwraca uwagę na: procedury bezpiecznego rejestrowania, identyfikację i uwierzytelnianie użytkowników, system zarządzania hasłami, korzystanie z narzędzi systemowych, zamykanie sesji po określonym czasie, ograniczanie czasu trwania połączenia.
Przetwarzanie mobilne i praca na odległość. Zagadnienie to dla bezpieczeństwa informacji w sieci ma szczególne znaczenie. Norma PN-ISO/IEC 17799:2005 zwraca w tym zakresie uwagę nie tylko na konieczność zabezpieczenia transmisji danych między urządzeniami mobilnymi a systemem centralnym administratora danych, ale również na okoliczność kradzieży czy zagubienia tych urządzeń.

Pozyskiwanie, rozwój i utrzymanie systemów informacyjnych

W rozdziale tym omawiane są m.in.:

- zabezpieczenia kryptograficzne (w tym polityka korzystania z zabezpieczeń kryptograficznych, zarządzanie kluczami),
- bezpieczeństwo w procesach rozwojowych i obsługi informatycznej (w tym: procedury kontroli zmian, techniczny przegląd aplikacji po zmianach w systemie operacyjnym, ograniczenia dotyczące zmian w pakietach oprogramowania, środki ograniczające wyciek informacji, prace rozwojowe nad oprogramowaniem powierzone firmie zewnętrznej),
- zarządzanie podatnościami technicznymi, w tym testowanie nowych wersji aplikacji i usług wprowadzanych do systemu. Odpowiednie procedury zarządzania tymi procesami mają duże znaczenie ze względu na fakt, że dostawcy oprogramowania są często pod znacznym naciskiem, aby wydawać poprawki tak szybko, jak to możliwe. Z tego powodu poprawka może w wystarczający sposób nie rozwiązywać problemu oraz mieć negatywne skutki uboczne, w tym wprowadzać nowe, nieznane dotychczas zagrożenia. Ponadto, w niektórych przypadkach, po zainstalowaniu poprawki jej odinstalowanie może być utrudnione, toteż dla zapewnienia bezpieczeństwa tych procesów niezbędne jest stosowanie w tym zakresie odpowiednich procedur.

Przy budowie systemu zabezpieczenia przetwarzanych danych można posłużyć się również innymi dokumentami i procedurami. Proces ten może być również podzielony na kilka etapów w zależności od zastosowanej metodyki i doświadczenia osób, które go przeprowadzają.

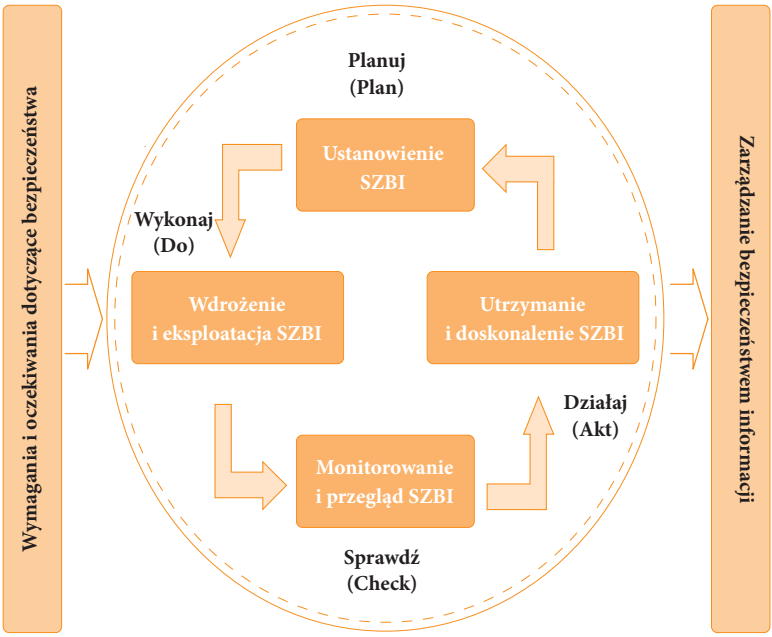
Dla systemu bezpieczeństwa informatycznego ważne jest również, aby raz opracowane procedury i środki były na bieżąco monitorowane i aktualizowane ze względu na zmieniające się technologie i nowe metody ataków na bezpieczeństwo, w tym nowe źródła zagrożeń. Politykę bezpieczeństwa należy również aktualizować, biorąc pod uwagę wła-

sne doświadczenia i obserwacje, a zwłaszcza te, dotyczące zaistniałych incydentów i prób naruszenia bezpieczeństwa. Po każdym zaistniałym incydencie naruszenia bezpieczeństwa lub odnotowanej próbie takiego naruszenia, zastosowane procedury powinny zostać przeanalizowane i uzupełnione o elementy, które będą wzmacniać ochronę przetwarzanych danych. Zadanie to administrator systemu, w którym przetwarzane są dane osobowe lub inne wartościowe dla przestępców dane, powinien objąć szczególnym priorytetem.

Z kolei administratorowi danych pomocne w wypracowaniu właściwych procedur bezpieczeństwa mogą być dokumenty normalizacyjne. Jednym z nich, określającym zasady eksploatacji, monitorowania, przeglądu, utrzymania i doskonalenia systemu zarządzania bezpieczeństwem informacji (SZBI)[39], jest norma „PN-ISO/IEC 27001:2007. *Technika informatyczna – Systemy zarządzania bezpieczeństwem informacji – Specyfikacja i wytyczne do stosowania*". Dokument ten zwraca uwagę na fakt, że wprowadzenie SZBI powinno być dla organizacji decyzją strategiczną ze względu na jej potrzeby i cele biznesowe, wymagania bezpieczeństwa, realizowane procesy oraz wielkość i strukturę organizacyjną. W normie tej zastosowano podejście procesowe w celu ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i doskonalenia SZBI. Norma PN-ISO/IEC 27001:2007 stosuje znany już dobrze model – Planuj – Wykonaj – Sprawdź – Działaj (PDCA), który jest stosowany do całej struktury procesów zarządzania bezpieczeństwem (Rys. 3).

[39] W literaturze z zakresu zarządzania bezpieczeństwem informacji równolegle ze skrótem SZBI operuje się skrótem ISMS (*Information Security Management System*).

Zasada: Planuj - Wykonaj - Sprawdź - Działaj



Rys. 3. Schemat zarządzania bezpieczeństwem wg PN-ISO/IEC 27001 – Zasada: Planuj – Wykonaj – Sprawdź – Działaj.

Norma PN-ISO/IEC 27001:2007 dzieli wymagane zabezpieczenia na 11 następujących obszarów:

- polityka bezpieczeństwa,
- organizacja bezpieczeństwa informacji,
- zarządzanie aktywami,
- bezpieczeństwo zasobów ludzkich,
- bezpieczeństwo fizyczne i środowiskowe,
- zarządzanie systemami i sieciami,

- kontrola dostępu,
- pozyskiwanie, rozwój i utrzymanie systemów informatycznych,
- zarządzanie incydentami związanymi z bezpieczeństwem informacji,
- zarządzanie ciągłością działania,
- zgodność (z przepisami prawnymi, politykami bezpieczeństwa i standardami, wymaganiami audytu).

Dużą zaletą normy jest kompleksowe podejście do bezpieczeństwa informacji. Omawia ona obszary bezpieczeństwa fizycznego, osobowego, teleinformatycznego oraz prawnego. Ze względu na kompleksowe podejście do tematu bezpieczeństwa informacji oraz ogólny charakter wymagań, może być podstawą budowy SZBI zarówno w małych organizacjach, jak i wielkich koncernach, a także dotyczyć różnych sektorów branżowych.

9.4. Instrukcja zarządzania systemem informatycznym

Wymienione wyżej elementy zarządzania bezpieczeństwem powinny zostać uwzględnione w instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, o której mowa w § 3 i § 5 rozporządzenia. Instrukcja ta, zgodnie z § 5 rozporządzenia, powinna zawierać ogólne informacje o systemie informatycznym i zbiorach danych osobowych, które są przy ich użyciu przetwarzane, zastosowane rozwiązania techniczne, a także procedury eksploatacji, jakie wprowadzono w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych. W przypadku gdy administrator danych wykorzystuje nie jeden, lecz kilka systemów informatycznych, powinien opracować jedną, ogólną instrukcję zarządzania lub oddzielną dla każdego z systemów. W pierwszym rozwiązaniu instrukcja zarządzania powinna opisywać zarówno wspólne dla wszystkich systemów rozwiązania oraz przyjęte procedury, jak i te specyficzne dla każdego z nich.

W instrukcji zarządzania systemem informatycznym powinny być wskazane systemy informatyczne, których ona dotyczy, ich lokalizacje, stosowane metody dostępu (bezpośrednio z komputera, na którym system jest zainstalowany, w lokalnej sieci komputerowej albo poprzez sieć telekomunikacyjną, np. łącze dzierżawione, Internet). Instrukcja powinna obejmować wszystkie najważniejsze zagadnienia dotyczące zarządzania bezpieczeństwem informacji, a w szczególności elementy wymienione w § 5 rozporządzenia, na które składają się:

1) *procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności,*
2) *stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem,*
3) *procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu,*
4) *procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania,*
5) *sposób, miejsce i okres przechowywania:*
   a) *elektronicznych nośników informacji zawierających dane osobowe,*
   b) *kopii zapasowych, o których mowa w pkt. 4,*
6) *sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia,*
7) *sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 rozporządzenia,*
8) *procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.*

W celu zapewnienia ochrony przetwarzanym danym, w odniesieniu do każdego z wymienionych wyżej punktów, w treści instrukcji powinny być wskazane zasady postępowania odpowiednie dla stosowanych systemów informatycznych.

10. Środki ochrony użytkowników indywidualnych przed zagrożeniami bezpieczeństwa w sieci

Korzystając z Internetu w pracy czy w domu, przesyłamy wiele dokumentów w formie elektronicznej. Coraz więcej poufnych informacji przechowujemy na dyskach twardych komputerów podłączonych do Internetu. Często są to dane, których przechwycenie przez cyberprzestępców może wyrządzić dużą szkodę. Dlatego szczególną uwagę należy zwrócić na zabezpieczenie komputera podłączonego do Internetu.

Dostęp do komputera powinien być zabezpieczony odpowiednio złożonym hasłem, aby nie było łatwe do odgadnięcia lub „złamania". Hasło powinno się składać ze znacznej liczby ilości znaków, w tym znaków specjalnych, cyfr, dużych i małych liter. W przypadku gdy mamy dostęp np. do systemu bankowego, administrator systemu stosuje dodatkowe mechanizmy bezpieczeństwa, takie jak maskowanie hasła, które polega na tym, że użytkownik przy każdej próbie logowania podaje tylko część hasła, wskazaną przez system. W celu zwiększenia bezpieczeństwa dostępu hasło powinno być co pewien czas zmieniane.

Oprócz hasła ważnym elementem zabezpieczenia komputera jest oprogramowanie antywirusowe, które zabezpiecza komputer przed pobraniem zainfekowanych plików danych lub plików z programami z poczty elektronicznej bądź innych źródeł (np. odwiedzanych stron www, innych komputerów w sieci P2P, nośników danych tupu USB). Ocbrona przed atakami na oprogramowanie systemowe, niektórymi typami robaków, próbami włamań i skanowania portów wymaga użycia specjalnych systemów ochrony typu *firewall*[40].

Ponadto na stacjach komputerowych wykorzystywanych do łączenia się z Internetem warto stosować:

[40] *Firewall* (z ang. ściana ogniowa) – pojecie to odnosi się do systemu zabezpieczeń komputerów lub całych sieci lokalnych przed zagrożeniami z sieci zewnętrznej jak i wewnętrznej. Do jego podstawowych funkcji należy ograniczanie dostępu z zewnątrz tylko do usług i podmiotów, dla których są niezbędne.

- wyłącznie legalne oprogramowanie i przestrzegać zaleceń producentów,
- najnowsze uaktualnienia systemowe,
- oprogramowanie antywirusowe z aktualizowanymi na bieżąco bazami wirusów,
- zaporę ogniową (ang. *firewall*), co pozwoli na stałe monitorowanie i rejestrowanie informacji napływających z zewnątrz, ostrzega również, jeśli program z używanej stacji komputerowej spróbuje wysłać informacje na zewnątrz; korzystanie z tego typu programów wymaga wyższego stopnia znajomości systemu zainstalowanego na komputerze, aby wiedzieć, które programy mogą mieć dostęp do Internetu, a które nie,
- odpowiednio złożone hasła dostępu.

Zawsze jednak należy pamiętać, że jednym z najskuteczniejszych narzędzi walki z zagrożeniami, w tym szczególnie z zagrożeniami typu *phishing* i *pharming*, jest ciągła edukacja użytkowników mająca na celu podnoszenie ich świadomości o istniejących w Internecie zagrożeniach, mechanizmach działania przestępców komputerowych, nowych metodach ataków itp. Ciągłość takiej edukacji jest niezbędna zarówno z uwagi na szybkie zmiany w technologii, jak i nowe metody działania przestępców, które tę technologię wykorzystują. Niezależnie od tego konieczne jest utrwalenie w świadomości użytkowników pewnych „żelaznych" zasad postępowania z pocztą elektroniczną i innymi źródłami informacji, a mianowicie takich, że:

1) Nigdy nie należy ufać nadawcy e-maila, który nie jest podpisany elektronicznie! Istnieje możliwość spreparowania e-maila tak, by sprawiał wrażenie, że wysłała go osoba lub przedstawiciel instytucji, którą się zna i której się ufa. Szacuje się, że w ponad 95% ataków używa się podrobionych adresów lub skradzionych adresów e-mail, aby wiadomość sprawiała wrażenie autentycznej.

2) Zawsze należy uważnie sprawdzać zawartość e-maila! Zdarza się, że twórca *phishingowego* e-maila zamieszcza cały tekst jako obrazek, po kliknięciu w który następuje przekierowanie do oszukańczej strony, której adres nie jest widoczny w treści wiadomości.
3) Nie należy uruchamiać załączników do poczty elektronicznej, jeżeli nie ma się pewności, że jest to załącznik bezpieczny. Pod postacią załączników *phisherzy* często wysyłają wirusy lub inne programy, których zadaniem jest doprowadzenie do kradzieży ważnych informacji. Szacuje się, że aż około 90% wirusów rozpowszechnianych jest poprzez e-mail.
4) Należy używać programu antywirusowego oraz oprogramowania wykrywającego i usuwającego oprogramowanie szpiegujące i złośliwe typu *spyware* i *malware*. Oprogramowanie antywirusowe i inne systemy zabezpieczeń należy regularnie aktualizować.
5) Regularnie trzeba aktualizować swój system operacyjny przy pomocy łatek i uaktualnień pobranych ze strony producenta systemu.
6) Nigdy nie należy wysyłać e-mailem żadnych danych osobistych typu hasła, numery identyfikacyjne, numery kart kredytowych! Żaden bank ani inna instytucja finansowa nigdy nie proszą o wysyłanie takich danych pocztą elektroniczną. Jeśli nawet pojawią się jakieś problemy z kontem, użytkownik powiadamiany jest o tym w sposób określony w regulaminie, zwykle telefonicznie, osobiście poprzez konsultanta lub listownie.
7) Należy zwracać uwagę na adres strony internetowej, a dla zachowania bezpieczeństwa wpisywać go ręcznie. W gotowych linkach przesłanych pocztą elektroniczną może kryć się pułapka w postaci przekierowania na fałszywą stronę docelową.
8) Należy używać przeglądarek internetowych, które zajmują wysokie lokaty w testach bezpieczeństwa. W celu uzyskania dostępu do serwisu zawierającego informacje poufne należy używać tylko przeglądarek, które są rekomendowane przez dostawcę danego serwisu.
9) Przed podaniem na stronie internetowej swoich poufnych danych (takich jak np. identyfikator i hasło do serwisu bankowego) należy

upewnić się, samodzielnie lub za pomocą odpowiedniego oprogramowania, do kogo rzeczywiście należy dana strona internetowa.

10) Regularnie należy odwiedzać serwisy poświęcone *phishingowi*, takie jak www.antiphishing.org/; phishing.org/, www.nophishing.org/, millersmiles.co.uk itp. Dzięki temu użytkownik będzie na bieżąco uzupełniał swoją wiedzę o nowych metodach działania przestępców, a *phisherzy* będą mieli mniejsze szanse jego „złowienia".

W walce z *phishingiem* ważne jest również, aby uświadamiać użytkowników Internetu o potrzebie jak najaktywniejszego włączania się do niej po stronie poszkodowanych. Użytkownicy powinni być informowani o tym, gdzie i w jaki sposób można np. zgłosić podejrzaną o *phishing* stronę internetową. W przypadku instytucji finansowych klienci usług bankowości internetowej powinni być informowani o możliwości zgłaszania podejrzanych stron do odpowiednich służb bezpieczeństwa. Warto nadmienić, że niemal wszystkie instytucje finansowe udostępniają swoim klientom informacje o adresach poczty elektronicznej lub stronach internetowych, poprzez które można je powiadomić o napotkanych, podejrzanych witrynach. MasterCard podaje w tym celu adres: scams@fraudwatchinternational.com, Visa adres: phishing@visa.com. Informacje o napotkaniu witryn podejrzanych o wyłudzanie danych można przesłać również do innych organizacji zajmujących się zwalczaniem przestępczości komputerowej, np. do Anti-Phishing Working Group (APWG) – międzynarodowej grupy roboczej zajmującej się przestępczością komputerową z zakresu *phishingu*, *pharmingu* i kradzieży tożsamości elektronicznej na adres reportphishing@antiphishing.org.

Należy również pamiętać, że żadne z wyżej wymienionych zabezpieczeń nie ochroni naszych danych, jeśli wpiszemy je do portali społecznościowych lub innych dzielonych w sieci zasobów informacyjnych, które coraz częściej stają się celem ataków wielu grup przestępczych.

11. Pytania i odpowiedzi

11.1. Zabezpieczenie elektronicznych formularzy

Jakie zabezpieczenia i funkcjonalności wymagane są od systemu elektronicznej rejestracji poprzez Internet?

Przepisy ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych wymagają, aby systemy informatyczne używane do przetwarzania danych osobowych spełniały warunki umożliwiające administratorom danych zapewnienie bezpieczeństwa przekazywanych danych oraz ochrony praw i wolności osób, których dane dotyczą.

Warunki w zakresie zapewnienia bezpieczeństwa.

W przypadku przetwarzania danych osobowych przy użyciu komputerów mających połączenie z Internetem, a więc z siecią publiczną, zarówno system informatyczny używany do ich przetwarzania, jak i przetwarzane przy jego użyciu dane są narażone na różne zagrożenia w sposób szczególny.

Stąd też, zgodnie z § 6 ust. 4 rozporządzenia ministra spraw wewnętrznych i administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. nr 100, poz. 1024), nazywanego dalej rozporządzeniem, administrator danych obowiązany jest w takim przypadku zastosować środki bezpieczeństwa na poziomie wysokim.

W praktyce oznacza to, że system używany przez administratora do przetwarzania danych osobowych przy użyciu formularza dostępnego poprzez Internet powinien spełniać wszystkie minimalne wymagania określone w załączniku do rozporządzenia dla zabezpieczeń na poziomie podstawowym, podwyższonym oraz wysokim.

Przede wszystkim powinien być zabezpieczony przed zagrożeniami z sieci publicznej poprzez zastosowanie środków chroniących go przed nieuprawnionym dostępem, które zapewniają kontrolę przepływu informacji między tym systemem a siecią publiczną oraz kontrolę działań inicjowanych z sieci publicznej (punkt XII załącznika do rozporządzenia). Ponadto transmisja danych między systemem administratora a komputerem rejestrującego się użytkownika powinna być zabezpieczona przy użyciu kryptograficznych środków ochrony danych (np. poprzez zastosowanie protokołu SSL). Hasła osób będących użytkownikami części systemu, w którym przetwarzane są dane pozyskane poprzez formularz, jak również innymi drogami, powinny mieć długość co najmniej 8 znaków oraz zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.

Niezależnie od wyżej wymienionych, minimalnych środków bezpieczeństwa określonych w rozporządzeniu, administrator powinien zastosować inne, dodatkowe środki bezpieczeństwa ograniczające zagrożenia bezpieczeństwa zidentyfikowane w wyniku analizy ryzyka przeprowadzonego przez administratora danych dla środowiska informatycznego, w którym użytkowany jest jego system informatyczny.

Warunki w zakresie zapewnienia praw i wolności osób, których dane dotyczą.

W zakresie dotyczącym zapewnienia ochrony praw i wolności osób, których dane dotyczą, system używany przez administratora danych osobowych, zgodnie z art. 32 i 38 ustawy, powinien z kolei zapewniać funkcjonalność umożliwiającą sprawowanie kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane. Szczegóły w zakresie wymagań funkcjonalnych systemu informatycznego używanego do przetwarzania danych osobowych zawarte są w § 7 rozporządzenia, który brzmi:

1. *Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym — z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu*

w celu udostępnienia go na piśmie — system ten zapewnia odnotowanie:

1) *daty pierwszego wprowadzenia danych do systemu;*
2) *identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba;*
3) *źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą;*
4) *informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych;*
5) *sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy.*

2. *Odnotowanie informacji, o których mowa w ust. 1 pkt 1 i 2, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.*
3. *Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust. 1.*

Należy jednak pamiętać, że wymienione wymagania funkcjonalne odnoszą się do całości systemu informatycznego używanego do przetwarzania danych, który w przypadku systemów umożliwiających pozyskiwanie danych za pośrednictwem formularza na stronie internetowej składa się z części obsługującej formularz oraz z części obsługującej dane zebrane przy użyciu formularzy. Specyfiką takich systemów jest to, że osobami wprowadzającymi dane do systemu nie są użytkownicy obsługujący tę część systemu, w której przechowywane są dane pozyskane z formularzy, których wskazał administrator danych, ale osoby nieznane administratorowi, które samodzielnie wpisują w udostępniony formularz dane ich dotyczące i wysyłają je do administratora danych. Rozwiązanie takie nie umożliwia na etapie pozyskiwania danych zapewnienia kon-

troli nad tym, kto wprowadził dane, o której mowa w art. 38 ustawy, jeżeli przekazywane w formularzu dane nie są podpisywane przy użyciu podpisu elektronicznego. Dlatego w opisanym wyżej przypadku, jeśli przekazane dane nie są opatrzone podpisem elektronicznym, dodatkową weryfikację danych, które zostały wprowadzone do systemu, powinien przeprowadzać administrator, np. weryfikując je w czasie, kiedy osoby te zgłoszą się do niego osobiście (np. podczas szkolenia/konferencji) lub w inny sposób.

Innym warunkiem funkcjonalności systemu, o którym mowa wyżej, jest to, aby wobec osób, które będą się rejestrować przy użyciu „wystawionego" w Internecie formularza, spełniony był tzw. obowiązek informacyjny. Zatem osoba, która zamierza dokonać rejestracji przy użyciu danego formularza, powinna być poinformowana o tym, kto jest administratorem danych, w jakim celu przekazane dane będą przetwarzane, a także o dobrowolności albo obowiązku podania danych, a jeśli taki obowiązek istnieje – o jego podstawie prawnej oraz o prawach i obowiązkach osób, których dane są przetwarzane, wynikających z ustawy o ochronie danych osobowych. Ponadto w opisanym przypadku, zgodnie z art. 24 ust. 1 pkt 2 ustawy, powinny być przekazane również informacje o odbiorcach lub kategoriach odbiorców danych.

W przypadku, gdy podmiot udostępniający formularz, jest usługodawcą w rozumieniu art. 2 pkt 6 ustawy z 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. nr 144 poz. 1204 z późn. zm.), wówczas spełnić powinien dodatkowo również wszystkie warunki wynikające z tej ustawy, tj. warunki określone w art. 7 pkt 1 dotyczące funkcjonalności oraz warunki określone w art. 8 pkt 1 ppkt 2 w zakresie dotyczącym publikacji regulaminu świadczenia usług.

11.2. Infrastruktura telekomunikacyjna a dane osobowe

Czy zakres numeracji aktywnej obsługiwanej przez Przełącznice Główne (PG) operatora telekomunikacyjnego opisany nazwami poszczególnych ulic, numerami domów wraz z numeracją

lokali, można uznać za dane osobowe w rozumieniu ustawy o ochronie danych osobowych?

Informacji obejmujących zakres numeracji aktywnej obsługiwanej przez Przełącznice Główne (PG) operatora telekomunikacyjnego opisanych nazwami ulic, numerami domów i numerami lokali, nie można uznać za dane osobowe, ponieważ w żaden sposób nie umożliwiają dokonania identyfikacji osoby fizycznej. Przetwarzanie informacji, o których mowa wyżej, mające na celu ewidencjonowanie zasobów sieci telekomunikacyjnej i wykorzystywanie jej w celach obsługi infrastruktury technicznej, nie powoduje, że możliwe staje się zidentyfikowanie osoby, która zamieszkuje w danej strefie numeracyjnej, a nawet korzysta z konkretnego punktu abonenckiego. Identyfikacja osoby byłaby możliwa wyłącznie wówczas, gdyby informacje te zawierały dodatkowo np. numer abonenta, numer telefonu abonenta czy imię i nazwisko abonenta.

Ponadto z treści pytania nie wynika, jaki potencjalny związek miałby istnieć między wskazaną nieruchomością a ewentualną osobą, której dane miałyby być przetwarzane. Toteż z punktu widzenia technicznego, korzystając z informacji zawartych w wymienionym zbiorze danych, nie jest możliwe zidentyfikowanie osoby fizycznej, bez podania takiego związku. Zgodnie bowiem z interpretacją pojęcia „dane osobowe" zawartą w Opinii 4/2007 Grupy Roboczej art. 29 ds. ochrony danych osobowych w sprawie pojęcia danych osobowych przyjętej 20 czerwca 2007 r., jednym z warunków, jakie muszą spełniać dane osobowe, jest związek określonej informacji z osobą. Związek ten może być ustalony na podstawie treści informacji (informacje na temat danej osoby), celu wykorzystywania informacji (np. ocena danej osoby) lub skutku, jaki wywołuje określona informacja (np. wpływ na prawa i interesy określonej osoby). Związek danej informacji z osobą, której ona dotyczy, może być ustalony również na podstawie danych o źródle ich pochodzenia lub danych uzyskanych z tego źródła.

W pytaniu nie pojawiła się żadna informacja, która wskazywałaby jednoznacznie na jakikolwiek związek wymienionych danych z potencjalną osobą, której dane te miałyby dotyczyć. Informacja o numerze domu i numerze lokalu nie daje takiego związku, jeśli się nie dookreśli,

czy chodzi o właściciela danego lokalu, czy lokatora, który w nim zamieszkuje. Dlatego należy uznać, że w okolicznościach wskazanych w pytaniu określone tam dane nie są danymi osobowymi w rozumieniu art. 6 ustawy o ochronie danych osobowych.

11.3. Zabezpieczenia stosowane przez osoby kontaktujące się z instytucjami przez skrzynkę kontaktową

Czy osoby kontaktujące się z publicznym lub prywatnym podmiotem poprzez system elektronicznej skrzynki kontaktowej muszą bezwzględnie stosować wysoki poziom bezpieczeństwa wymagany przepisami o ochronie danych osobowych i zmieniać hasło co najmniej raz w miesiącu? Jak często ma odbywać się zmiana hasła w przypadku, gdy przeciętny użytkownik loguje się do ww. systemu teleinformatycznego danego podmiotu średnio raz na rok?

Warunki, jakim powinien odpowiadać system informatyczny używany do przetwarzania danych osobowych, w tym minimalną częstotliwość zmiany haseł określa rozporządzenie ministra spraw wewnętrznych i Administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. W § 2 tego rozporządzenia zdefiniowano pojęcie „identyfikator użytkownika" jako ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych przy użyciu danego systemu informatycznego. Pod pojeciem tym rozumie się również użytkownika systemu informatycznego jako osobę upoważnioną do przetwarzania danych. Pojęcie to może się odnosić do:

1) osoby upoważnionej przez administratora danych, do przetwarzania danych w jego imieniu, tj. osoby, która ma dostęp do przetwarzania informacji o różnych osobach z danego zbioru danych, lub
2) osoby, której administrator umożliwił samodzielne zarejestrowanie się w systemie i wprowadzenie tylko swoich własnych danych.

W pierwszym przypadku przetwarzanie danych wiąże się z posiadaniem uprawnień dostępu do określonej kategorii informacji o osobach, których dane są przetwarzane i/lub dostępu do informacji o określonej grupie osób. Przetwarzanie takie wiąże się z przyjęciem przez użytkownika odpowiedzialności w zakresie wykonywanych operacji na danych osobowych określonej grupy osób. Jednocześnie odpowiedzialność za wszelkie nieprawidłowości powstałe w wyniku nienależycie czy też niezgodnie z prawem wykonanych operacji przetwarzania, ponosić może zarówno administrator danych, jak i osoba przez niego upoważniona. Działania związane z nadawaniem identyfikatorów takim użytkownikom i zachowaniem poufności ich haseł mają na celu zapewnienie rozliczalności wykonywanych operacji, a także uniemożliwienie dostępu do danych osobom nieuprawnionym. Należy tutaj podkreślić, że użytkownicy tej kategorii to najczęściej osoby zatrudnione u administratora danych lub w podmiocie, któremu powierzono przetwarzanie.

W drugim przypadku osoba, która staje się użytkownikiem systemu na skutek samodzielnego zarejestrowania się, uzyskuje wyłącznie uprawnienia do przetwarzania swoich własnych danych. Często uprawnienia te są ograniczone, np. do utworzenia wpisu (zarejestrowania się), jego modyfikacji, ale bez praw do jego usunięcia.

Warto zauważyć, że ww. rozporządzenie nie rozróżnia wymienionych wyżej dwóch kategorii użytkowników. Przykładem tej ostatniej kategorii użytkowników jest coraz liczniejsza grupa osób korzystających z serwisów internetowych. Osoby te, nie są na ogół związane z dostawcami tych serwisów żadnym stosunkiem pracy. Jedynymi dokumentami, które regulują ich „współpracę" są, w większości przypadków, regulamin świadczenia usług, z którym użytkownicy powinni się zapoznać i stosować w praktyce, oraz polityka prywatności, w której dostawca usługi informuje o zakresie i celach przetwarzania danych. W dokumentach tych dostawca usługi przedstawia się i informuje użytkowników o ich prawach i obowiązkach, wypełniając w ten sposób obowiązek informacyjny. Zakres uprawnień takich użytkowników jest na ogół ograniczony wyłącznie do przetwarzania ich własnych danych. Dopuszczenie użytkowników tej kategorii do przetwarzania własnych danych (wpro-

wadzania, modyfikacji) stanowi w tym przypadku ułatwienie dla administratora danych w wypełnianiu wymogów art. 32 ust. 1 ustawy, a zwłaszcza jego punktów 2 i 6.

Biorąc pod uwagę bezpieczeństwo przetwarzania w systemie informatycznym, administrator danych, zgodnie z wymogami ustawy o ochronie danych osobowych i wspomnianego wyżej rozporządzenia, powinien zapewnić poufność przetwarzanych danych (art. 36 ustawy) poprzez zastosowanie w systemie informatycznym odpowiednich mechanizmów kontroli dostępu. W przypadku, gdy mechanizmy te wykorzystują jedynie identyfikator użytkownika i hasło, administrator danych ma obowiązek zapewnić, aby stosowane hasła miały odpowiednią składnię (długość i różnorodność używanych znaków) oraz były okresowo zmieniane (punkty IV.1, IV.2 oraz VIII do załącznika do rozporządzenia).

Niemniej zastosowanie rozwiązania umożliwiającego samodzielne wprowadzanie danych do systemu, ich modyfikowanie, uzupełnianie bądź usuwanie odbywa się kosztem utraty przez administratora pełnej kontroli nad procesem przetwarzania. W przypadku bowiem, kiedy administrator danych daje nieznanym sobie osobom uprawnienia w systemie do samodzielnego utworzenia sobie konta z uprawnieniami do wpisywania i edycji danych, bez weryfikacji, czy wprowadzone dane są zgodne ze stanem faktycznym, występuje sytuacja, w której w chwili wprowadzania danych nie jest spełniony warunek kontroli nad tym, kto je do systemu wprowadził (art. 38 ustawy). Inną konsekwencją takiego rozwiązania są ograniczone możliwości kontroli takich użytkowników w zakresie stosowania wymaganych procedur bezpieczeństwa, w tym zmiany hasła z częstotliwością co najmniej raz na 30 dni.

Biorąc pod uwagę, że stosownie do art. 36 ust. 1 ustawy, „administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną…", należy zauważyć, że dla wspomnianej grupy użytkowników internetowych, mających dostęp jedynie do swoich własnych danych, przechwycenie hasła przez nieuprawnioną osobę może skutkować jedynie utratą kontroli nad ich własnymi danymi. Porównując zagrożenia

i ryzyko uzyskania dostępu do systemu informatycznego z poziomu użytkownika upoważnionego przez administratora danych (np. osoby u niego zatrudnionej), który ma uprawnienia do przetwarzania danych dotyczących wszystkich osób zgromadzonych w systemie oraz użytkownika internetowego, który ma uprawnienia tylko do swoich własnych danych, doskonale widać, że w tym ostatnim przypadku mamy do czynienia „jedynie" z możliwością utraty jego własnej tożsamości elektronicznej i nie wpływa to bezpośrednio na bezpieczeństwo całego systemu i zgromadzonych w nim danych innych użytkowników.

Rozpatrując zasadę stosowania zabezpieczeń stosownie do zagrożeń i ryzyka, w pełni uzasadnione wydaje się, aby w przypadku, kiedy administrator danych informuje takich „internetowych użytkowników" o obowiązku zmiany hasła z częstotliwością nie rzadziej niż co 30 dni, rozwiązanie takie uznać należy za wystarczające. Przepisy rozporządzenia nie nakazują bowiem, aby realizacja wymogu, o którym mowa w punkcie IV.2 załącznika do rozporządzenia, wspierana była przez administratora poprzez np. blokadę konta danego użytkownika czy też inne działania. Przepisy rozporządzenia, nie wprowadzając w powyższym zakresie żadnych wytycznych, pozwalają na własne inicjatywy administratora danych, które mogą polegać np. na przypominaniu użytkownikom o zagrożeniach, jakie może spowodować brak zmiany haseł albo na wprowadzeniu procedur, które po zidentyfikowaniu, że użytkownik nie zmieniał hasła przez okres dłuższy niż 30 dni, automatycznie wymuszą, aby zmiana taka została wykonana.

11.4. Zabezpieczenia stosowane przy połączeniu z siecią publiczną

Czy informatyczny system obsługi klientów, w którym: 1) baza danych osobowych zlokalizowana jest na serwerze sieci wewnętrznej (LAN), która połączona jest z siecią Internet poprzez systemy ochrony typu *firewall*, 2) serwer z bazą klientów odizolowany jest logicznie od sieci Internet, oraz 3) komputery użytkowników posiadają dostęp jedynie do poczty elektronicznej, wymaga zabezpieczeń na poziomie wysokim?

Rozpatrując przedstawioną powyżej problematykę, należy mieć na uwadze fakt, iż w myśl § 6 ust. 4 rozporządzenia ministra spraw wewnętrznych i administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. nr 100, poz. 1024), poziom wysoki stosuje się, gdy przynajmniej jedno urządzenie systemu informatycznego, służące do przetwarzania danych osobowych połączone jest z siecią publiczną.

W analizowanym przykładzie należy zauważyć, że serwer zawierający bazę danych osobowych systemu obsługi klientów podłączony jest do sieci wewnętrznej (LAN) posiadającej dostęp do sieci Internet. Z treści pytania wynika, że sam serwer, ze względu na separację logiczną (separację, którą zapewnia m.in. odpowiednia konfiguracja *routingu*, konfiguracja odpowiednich systemowych uprawnień dostępu itp.), nie posiada dostępu do sieci Internet. Dostęp do sieci Internet mają natomiast stacje komputerowe, na których użytkowany jest system obsługi klientów, jak również, o czym nie należy zapominać, dostęp do sieci Internet posiada urządzenie zapewniające logiczną separację serwera od sieci Internet. Dlatego należy uznać, że spełniony został warunek, o którym mowa w § 6 ust. 4 rozporządzenia, tj. przynajmniej jedno urządzenie systemu informatycznego, biorące udział w procesie przetwarzaniu danych, połączone zostało z siecią publiczną Internet.

Przedstawiony system przetwarzania danych wymaga zatem zabezpieczeń na poziomie wysokim. Należy bowiem mieć na uwadze fakt, że zastosowanie zabezpieczeń dostępu do sieci Internet, w postaci wdrożenia mechanizmów typu *firewall*, czy też korzystanie przez użytkownika jedynie z poczty elektronicznej, nie ma żadnego wpływu na klasyfikację poziomu bezpieczeństwa. Istotny jest wyłącznie fakt, że co najmniej jedno z urządzeń biorących udział w procesie przetwarzania danych posiada dostęp do sieci Internet, czyniąc to urządzenie podatnym na liczne zagrożenia płynące z tej sieci.

11.5. Minimalna zawartość informacyjna formularzy internetowych

Jakie minimalne informacje powinien zawierać formularz internetowy do pozyskiwania danych osobowych?

Jedną z podstawowych zasad przetwarzania danych osobowych jest zasada tzw. minimalizacji danych, która oznacza, że administrator powinien przetwarzać tylko te dane osobowe, które są niezbędne z punktu widzenia celu, w jakim dane są przetwarzane. Zasada ta zabrania zbierania danych „na zapas", tj. w szerszym zakresie niż wymagane minimum.

Zgodnie bowiem z treścią art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych, administrator danych powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a zwłaszcza jest obowiązany zapewnić, aby dane te były adekwatne w stosunku do celów, w jakich są przetwarzane.

Pozyskiwane za pośrednictwem formularza internetowego dane osobowe powinny być ograniczone do niezbędnego minimum. Powinien on jednak zawierać takie pola, które umożliwią osobie, której dane dotyczą, wyrażenie zgody na przetwarzanie jej danych osobowych (jeżeli podstawą przetwarzania jest ta właśnie przesłanka legalności), oraz – w sytuacji, gdy administrator zamierza przetwarzać pozyskane dane także dla celów marketingowych – pole, za pomocą którego możliwe będzie wyrażenie (lub niewyrażenie) przez osobę, której dane dotyczą, zgody na przetwarzanie danych w takich właśnie celach.

Jednocześnie należy podkreślić, że zgoda na przetwarzanie danych osobowych powinna odnosić się do skonkretyzowanego stanu faktycznego i precyzować sposób i cel, w jakim pozyskane dane będą przetwarzane. Powyższe stanowisko potwierdził Naczelny Sąd Administracyjny, który w uzasadnieniu wyroku z 4 kwietnia 2003 r. (sygn. akt II SA 2135/02) orzekł, iż „(...) wyrażający zgodę musi mieć w momencie jej zawarcia świadomość tego, co kryje się pod tym pojęciem." Dalej czytamy również, że „(...) zgoda musi mieć charakter wyraźny, a jej wszystkie aspekty muszą być jasne dla podpisującego w momencie jej wyrażania."

Mając to na uwadze należy pamiętać, że formularze internetowe powinny przy polu umożliwiającym wyrażenie zgody na przetwarzanie danych zawierać dokładny, niebudzący wątpliwości opis sposobu i celu przetwarzania danych oraz informacje o zamiarze ewentualnego udostępniania danych innym podmiotom.

W przypadku, gdy zbierane dane osobowe administrator zamierza wykorzystywać dla celów marketingowych, w formularzu powinno być wyraźnie oddzielone pole na wyrażenie zgody na przetwarzanie danych od pola na wyrażenie zgody na przetwarzanie danych dla celów marketingowych.

Niedozwolone jest jakiekolwiek uzależnianie możliwości wysłania formularza i wyrażania zgody, np. na jednorazowy kontakt z administratorem (np. dotyczący określonej oferty bankowej) od wyrażenia zgody na „ogólne" przetwarzanie danych w celach marketingowych przez bliżej nieokreślony czas.

Administrator danych zobowiązany jest również do udzielenia osobie, której dane przetwarza, informacji wskazanych w art. 24 ust. 1 ustawy, tj. o adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna – o miejscu swojego zamieszkania oraz imieniu i nazwisku; celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych; prawie dostępu do treści swoich danych oraz ich poprawiania; dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej. Dlatego w systemie informatycznym służącym do przetwarzania danych osobowych, w przypadku, gdy dane są pozyskiwane za pomocą formularzy internetowych, dane o których mowa wyżej, powinny być zawarte bezpośrednio w formularzu lub bezpośrednio dostępne z tego formularza w postaci np. odwołania do innego dokumentu (polityki prywatności, regulaminu itp.), w którym informacje w powyższym zakresie są zawarte i zawsze dostępne.

IRON MOUNTAIN®

Bezpieczeństwo to stan, który daje poczucie pewności i gwarancje jego zachowania oraz szanse na doskonalenie. Jest to jedna z podstawowych potrzeb człowieka. Odznacza się brakiem ryzyka utraty czegoś dla człowieka szczególnie cennego – życia, zdrowia, pracy, szacunku, uczuć, dóbr materialnych i dóbr niematerialnych

Zagrożenie - zjawisko wywołane działaniem sił natury bądź człowieka, które powoduje, że poczucie bezpieczeństwa maleje bądź zupełnie zanika.

Iron Mountain to lider w dziedzinie ochrony i przechowywania informacji, obsługujący ponad 100 000 Klientów na całym świecie.

Iron Mountain Polska Sp. z o.o.

ul. Regulska 2, Reguły k/ Warszawy
05-820 Piastów
tel. (22) 753 61 41
fax (22) 753 61 43

www.ironmountain.pl

Dotychczas w serii
„ABC ochrony danych osobowych”
Biura Generalnego Inspektora Ochrony Danych Osobowych
ukazały się następujące publikacje:

- „ABC Ochrony danych osobowych”,
- „ABC Rejestracji zbiorów danych osobowych”,
- „ABC Wybranych zagadnień z ustawy o ochronie danych osobowych”,
- „ABC Zasad kontroli przetwarzania danych osobowych”,
- „ABC Zasad przekazywania danych osobowych do państw trzecich”,
- „ABC Zasad bezpieczeństwa przetwarzania danych osobowych przy użyciu systemów informatycznych”,
- „ABC Przetwarzania danych osobowych w sektorze bankowym”.

Wszystkie publikacje dostępne są na stronie
Generalnego Inspektora Ochrony Danych Osobowych

www.giodo.gov.pl

GIODO

Generalny Inspektor
Ochrony Danych Osobowych

Biuro Generalnego Inspektora
Ochrony Danych Osobowych

ul. Stawki 2, 00-193 Warszawa
tel. (0 22) 860 70 81
fax: (0 22) 860 70 86
kancelaria@giodo.gov.pl
www.giodo.gov.pl

edu GIODO
www.edugiodo.giodo.gov.pl