Janusz Figura[1]
Uniwersytet Ekonomiczny w Katowicach
Barbara Kos[2]
Uniwersytet Ekonomiczny w Katowicach

Bezpieczeństwo informacji jako element kształtowania łańcuchów dostaw operatorów logistycznych

1. WPROWADZENIE

Realizacja usług logistycznych i zapewnienie wysokiego poziomu ich jakości, związana jest oprócz fizycznego przemieszczania ładunków również z przepływem informacji. Jednakże niekontrolowany przepływ informacji dotyczących różnorodnych przedsięwzięć związanych zarówno z operacyjnymi, jak również strategicznymi działaniami operatorów usług logistycznych, w istotny sposób determinuje poziom bezpieczeństwa realizowanych łańcuchów dostaw. Tym gorzej, jeżeli działania na rzecz przepływu informacji mają celowo szkodliwy charakter, który skierowany jest na pozyskiwanie chronionych danych technologicznych, handlowych lub organizacyjnych operatorów logistycznych. Inżynieria bezpieczeństwa informacji wraz z rozwojem zaawansowanych technologii informatycznych, staje się obecnie jedną z kluczowych kwestii związanych z realizacją łańcuchów dostaw. Aktualnie wielu operatorów usług logistycznych boryka się z problemami zapewnienia właściwego poziomu bezpieczeństwa przepływu informacji. Celem artykułu jest zaprezentowanie wyników badań związanych z bezpieczeństwem informacji wśród operatorów usług logistycznych.

2. POJĘCIE BEZPIECZEŃSTWA INFORMACJI W ŁAŃCUCHU DOSTAW

Pojęcie bezpieczeństwa informacji stanowi kluczowy element sprawnego funkcjonowania łańcuchów dostaw operatorów logistycznych. Pojęcie bezpieczeństwa informacji jest złożonym i wieopłaszczyznowym zagadnieniem będącym przedmiotem zaintereowania wielu badaczy. W szerokim ujęciu można powiedziedzieć, że bezpieczeństwo informacji to stan lub proces, który gwarantuje istnienie operatorowi logistycznemu jego rozwój. Z tego punktu widzenia bezpieczeństwo informacji stanowi więc jeden z podstawowych elementów funkcjonowania operatora logistycznego, kształtując jednocześnie szanse i możliwości jego zmian w otoczeniu. Innymi słowy bezpieczeństwo informacji oznacza zwykle brak ryzyka utraty szczególnie cennego elementu, którym są zasoby informacyjne. Informacje stanowią więc szczególny rodzaj zasobów każdej organizacji, również operatorów realizujących usługi logistyczmne, choć z reguły najsłabiej chroniony. Warto również zaznaczyć, iż pojęcie bezpieczeństwa informacji znalazło odzwierciedlenie w międzynarodowej normie standaryzującej system zarządzania bezpieczeństwem informacji ISO 27001:2007 określającej wymagania związane z ustanowieniem, wdrażaniem, eksploatacją, monitorowaniem, przeglądem, utrzymaniem i doskonaleniem Systemu Zarządzania Bezpieczeństwem Informacji - PN-ISO/IEC 27001:2007[3]. Z punktu widzenia łańcuchów dostaw bezpieczeństwo informacji posiada zatem określoną wartość i jako takie powinno być właściwie chronione. Pojęcie bezpieczeństwa infromacji w łańcuchach dostaw, można więc zdefiniować jako zbiór działań, który podejmują jego uczestnicy dla zapewnienia ochrony dostępu przed nieuprawnionym dostępem, zniszczeniem, bądź modyfikacjom posiadających odpowiednie uprawnienia. Bezpieczeństwo informacji w łańcuchu dostaw posiada równiez swoje konotacje ekonomiczne, których wartość zdeterminowana jest nie tylko rzadkością

[1] janusz.figura@ue.katowice.pl
[2] bkos@ue.katowice.pl
[3] www.pkn.pl/certyfikacja-systemow-zarzadzania

występowania zasobów informacyjnych i kosztami ich pozyskiwania, ale zwłaszcza relacjami zachodzącymi w ramach wymiany usług logistycznych na rynku, określając - co, kto, ile, kiedy i jakich powinien dostarczać informacji dla sprawnej realizacji łańcucha dostaw.

3. POLITYKA BEZPIECZEŃSTWA INFORMACJI OPERATORÓW USŁUG LOGISTYCZNYCH

Realizacja łańcuchów dostaw wymaga od operatora usług logistycznych właściwego podejścia do polityki bezpieczeństwa niektórych zbiorów informacji, związanych zwłaszcza ze strategią rozwoju, informacjami finansowymi, jak również określonych danych chronionych z mocy prawa (dane osobowe, informacje niejawne itd.). Polityka bezpieczeństwa informacji jest więc zbiorem działań, które podejmuje oprataor usług logistycznych na rzecz ochrony informacji[4] określających metody i zasady pozwalające skutecznie zapewnić bezpieczeństwo ich przepływu w łańcuchu dostaw. Mówiąc szerzej jest to zbiór spójnych precyzyjnych i zgodnych z obowiązującym prawem przepisów reguł i procedur, według których kształtuje się przepływy zasobów informacyjnych operatora usług logistycznych. Punktem wyjscia do tworzenia bezpieczeństwa informacyjnego operatora usług logistycznych jest systematyzacja informacji zbiorów danych i sposobów ich przepływu, według kryteriów określajacych, które z nich i według jakiego stopnia powinny zostać chronione. Jak dotychczas w realizacji łańuchów dostaw wykształciły sie trzy poziomy polityki bezpieczeństwa informacji:

- poziom podstawowy obejmujący z jednej strony bezpieczeństwa informacji między innymi zakres prawny funkcjonowania polityki bezpieczeństwa, zdefiniowanie obszarów bezpieczeństwa informacji, ogólnych zasad i strategi bezpieczeństwa informacji, celów i zadań bezpieczeństwa informacyjnego, identyfikację struktury kanałów przepływów informacyjnych, zródeł informacji wyjściowej i wejściowej, przetwarzania i przechowywania informacji, struktury dostępu oraz z drugiej strony bezpieczeństwa systemu informatycznego operator usług logistycznych – regulamin sieci informatycznej (sposoby korzystania z sieci informatycznej, tryb dostępu, zasady przepływu informacji, zasady tworzenia kopii zapasowych, , identyfikacja osób odpowiedzialnych za funkcjonowanie sieci i jej poszczególnych elementów);
- poziom średni, którego istota koncentruje się na utworzeniu usystematyzowanych już zbiorach informacji, które należy sklasyfikować według stopnia ochrony, przypisując każdemu z nich odpowiednią metodę, cel i osobę odpowiedzialną za bezpieczeństwo informacji, przygotowanie zasad działania systemu informacyjnego w sytuacji kryzysowej;
- poziom najwyższy dotyczycący szczególnych sytuacji związanych z bezpieczeństwem informacji, w których może znaleźć się operator usług logistycznych; istotne jest przede wszystmi określenie zasad i sposobów ochrony informacji i reagowania na sytuacje kryzysowe, przeprowadzanie audytów bezpieczeństwa, jak również współpracy z zewnętrznymi interesariuszami, organizacjami i podmiotami, które wchodzą w inetrakcję z operatorem logistycznym, umożliwiając odpowiednie zabezpieczenie informacyjne.

Wskazane poziomy bezpieczeństwa informacji funkcjonujący wśród operatorów usług logistycznych posiadają najczęściej formę:

- regulaminów – opisujących zasady ochrony informacji, praw i obowiązków pracowników oraz zasad korzystania z poszczególnych środków technicznych przetwarzających informację,
- instrukcji – zestawów szczegółowych zasad i sposobów związanych z elementami, częściami polityki bezpieczeństwa informacji odniesionymi do określonych fragmentów, czasu i miejsca zastosowania,

[4] Informacja jest wszelkiego rodzaju treścią, przechowywaną na dowolnym nośniku informacji, wyrażoną za pomocą mowy, pisma, obrazu, rysunku, znaku, kodu, dźwięku lub w jakikolwiek inny sposób.

- procedur – opisujących szczegółowo postępowanie w określonych przypadkach zarówno w normalnym przepływie informacji, jak również w sytuacjach kryzysowych związanych z incydentem naruszenia bezpieczeństwa informacyjnego.

Polityka bezpieczeństwa informacji nastawiona jest na zabezpieczenie maksymalnego poziomu ochrony, który wynika z określonego przepływu informacji w łańcuchu dostaw, jednakże możliwie są sytuacje, w których zastosowane rozwiązania nie są w stanie zidentyfikować każdego z możliwych obszarów ryzyka bezpieczeństwa informacyjnego. Dlatego polityka bezpieczeństwa informacji koncetrować powinna się zwłaszcza na wyznaczeniu ryzyk nieakceptowanych. Ryzyko nieakceptowane oznacza sytuację, w której jakiś fragment bezpieczeństwa informacji związany z realizacją łańcucha dostaw jest najsłabiej chroniony, a istniejące regulaminy, instrukcje i procedury zabezpieczeń nie są w stanie zagwarantować dostatecznego poziomu bezpieczeństwa przepływu informacji. Dlatego też, polityka bezpieczeństwa informacji każdego operatora logistycznego, powinna zostać przygotowana również na tego typu ryzyko i w sposób elastyczny umożliwić:

- minimalizację ryzyka nieakceptowanego poprzez podejmowanie działań ograniczających źródła i czynniki mające wpływ na wystąpienie sytuacji danego poziomu ryzyka dla zagrożenia bezpieczeństwa informacji,
- unikanie ryzyka nieakceptowanego poprzez wzmocnienie możliwości zmianę stosowanych rozwiązań w organizacji i funkcjonowaniu bezpieczeństwa informacji poprzez zaprzestanie działań powodującej powstanie zagrożenia o danym poziomie przepływu informacji,
- transfer ryzyka nieakceptowanego - konieczność podjęcia działań mających na celu przekazanie odpowiedzialności w zakresie przepływu informacji i ich bezpieczeństwa na podmioty zewnętrzne.

Polityka bezpieczeństwa informacji operatorów logistycznych związana jest również z określonymi właściwościami, do których zalić należy:

- poufność – polega na tym, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom,
- integralność - właściwość zapewniająca dokładność i kompletność zasobów informacyjnych operatora usług logistycznych,
- dostępność – właściwość bycia dostępnym i użytecznym na żadanie opoważnionego iteresariusza, organizacji lub podmiotu współpracującego z operatorem usług logistycznych,
- autentyczność – właściwość polegajaca na tym, że pochodzenie lub zawartość informacyjna opisująca obiekt są takie jak deklarowane,
- rozliczalność – właściwość systemu informacyjnego pozwalająca przypisać określone działanie w systemie do osoby fizycznej lub procesu oraz umiejscowić w określonych ramach czasowych,
- niezaprzeczalność – brak możliwości zanegowania samego uczesntnictwa w całości lub części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie,
- niezawodność - właściwość oznaczająca spójne zamierzone zachowanie i skutki.

Polityka bezpieczeństwa stanowi istotne zagadnienie omawianej problematyki, jednakże nie jedyne. Dlatego spośród rozlicznych zagadnień, które związane są z zagadnieniem bezpieczeństwa informacji warto skoncetrować sie na dwóch aspektach, które będą stanowiły przedmiot dalszego popstępowania badawczego, a mianowicie na potrzebach bezpieczeństwa informacji oraz identyfikacji źródeł zagrożeń mających wpływ na bezpieczeństwo informacji w łańcuchu dostaw.

4. METODYKA BADAŃ

Celem przygotowanych i przeprowadzonych badań empirycznych było poznanie opinii respondentów tj. pracowników przedsiębiorstw sektora TSL na temat bezpieczeństwa informacji jako elementu kształtującego łańcuch dostaw. Szczególną uwagę zwrócono na dwa aspekty badanego zagadnienia a mianowicie na:

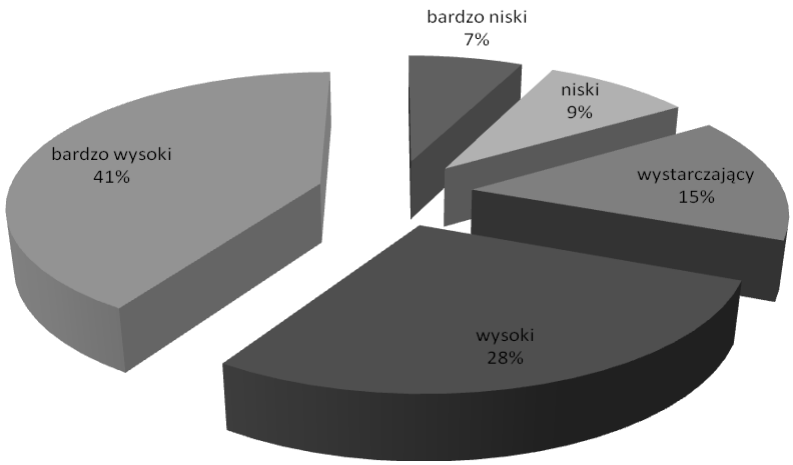
- dynamikę poziomu potrzeb bezpieczeństwa informacji w łańcuchu dostaw,

- identyfikację źródeł zagrożeń w mających wpływ na bezpieczeństwo informacji w łańcuchu dostaw,

Kwestionariusz składał się z pytań zamkniętych (z dobraną listą odpowiedzi w oparciu o studium literaturowe) jedno- i wielokrotnego wyboru. Dobór próby badawczej miał charakter celowy, co umożliwiło wybór respondentów o określonych cechach. Badanie przeprowadzono metodą kuli śnieżnej w grupie 42 operatorów usług logistycznych funkcjonujących na polskim rynku logistycznym. Do pomiaru i oceny bezpieczeństwa informacji wykorzystano pięciopunktową skalę (1 minimum – 5 maksimum). Czasokres badania obejmował drugi i trzeci kwartał 2014 roku. Ankieta stanowiła cenne źródło bezpośrednich informacji, która może wzbogacić wiedzę na temat badanego zagadnienia.

5. ANALIZA WYNIKÓW BADAŃ

Pierwszym aspektem badań nad bezpieczeństwem informacji w kształtowaniu łańcuchów dostaw było zagadnienie potrzeb ochrony informacji. Wyniki badań wyraźnie wskazują na bardzo wysoki oraz wysoki poziom potrzeb bezpieczeństwa informacji w łańcuchu dostaw, co wynika ze struktury udzielonych odpowiedzi. Pozytywnych odpowiedzi udzieliła grupa 69 % respondentów, jedynie 15 % uznała, że potrzeby bezpieczeństwa informacji są wystarczajace, 9%, że niskie i 7%, że bardzo niskie – rys. 1.



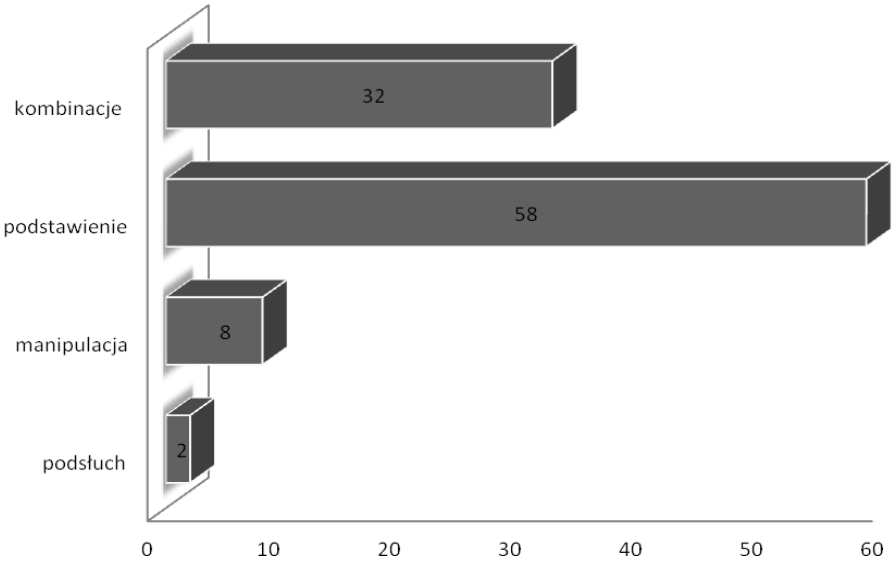
Rys. 1. Struktura poziomu potrzeb bezpieczeństwa informacji badanych operatorów usług logistycznych w łańcuchu dostaw.
Źródło: opracowanie na podstawie badań ankietowych.

Drugim aspektem badawczym było zagadnienie identyfikacji źródeł zagrożeń mających wpływ na bezpieczeństwo informacji w łańcuchu dostaw. Ponieważ identyfikacja źródeł zagrożeń stanowiła znaczący obszar badań, dlatego została sklasyfikowana na klika mniejszych grup według następujących kryteriów:

- zagrożenia zewnętrzne związane z przetwarzaniem bezpieczeństwa informacji,
- dane osobowe personelu operatora usług logistycznych,
- podatność sieci telekomunikacyjnych na zagrożenia dla bezpieczeństwa informacji,
- narzędzia programowe wykorzystywane do ataku na bezpieczeństwo informacji,
- technologie komputerowe, które mogą być wykorzystywane do kradzieży danych,
- stosowane socjotechniki w atakach na bezpieczeństwo informacji w sieci,
- obowiązki administratora sieci danych.

Zagrożenia związane z bezpieczeństwem informacji operatora usług logistycznych, wśród których na szczególną uwagę należy zwrócić na niebezpieczeństwa 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. W tej grupie największym zagrożeniem dla bezpieczeństwa informacji stanowią podstawienie 58 %, i kombinacje 32% (kombinacja - podstawienia, manipulacji, podsłuchu), najmniejszą grupę stanowią manipulacją 8 % i podsłuch 2 % - rys. 2. 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 sieciowych, a także staranności użytkowników w stosowaniu określonych zasad bezpieczeństwa informacji.

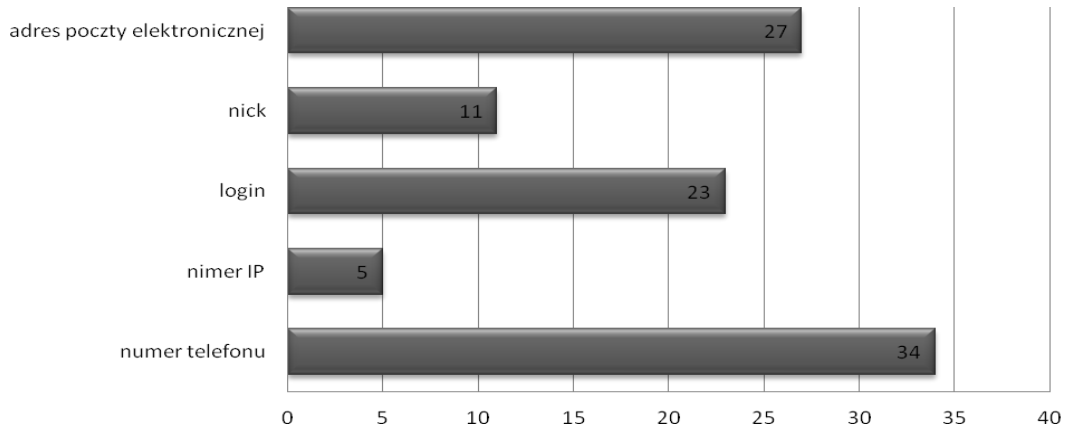


Rys.2. Struktura zagrożeń zewnętrznych bezpieczeństwa informacji zidentyfikowanych w badanej grupie operatorów usług logistycznych
Źródło: opracowanie na podstawie badań ankietowych

Klejnym ziedentyfikowanym źródłem zagrożeń jest bezpieczeństwo danych osobowych personelu operatora usług logistycznych. Za dane osobowe w myśl ustawy[5] 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. Warto zwrócić uwagę iż, użyte w cytowanej definicji kryterium oceny, jakie należy stosować przy przyznawaniu informacjom statusu danych osobowych, jest nieostre. Użyte w definicji sformułowanie „pośrednio" może być różnie rozumiane, chociażby co do liczby stopni pośrednictwa. Podobnie różnie w znaczeniu ilościowym można interpretować kryterium kosztów, czasu i działań[6]. 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

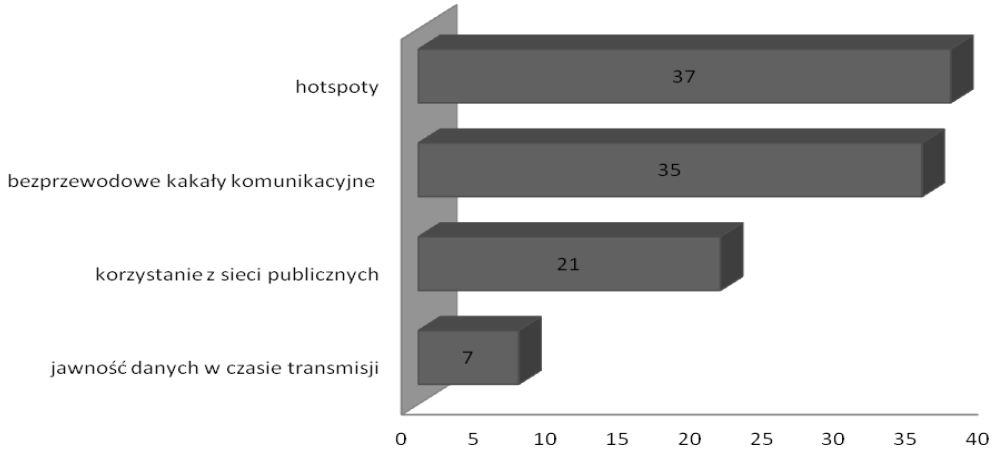
[5] Ustawa z dnia 29 sierpnia 2997 r. o ochronie danych osobowych. Dz.U. z 2002 r. nr 101, poz. 926 z późn. zm.), art.6.
[6] art. 6. us. 2 i 3 - Ustawa z dnia 29 sierpnia 2997 r. o ochronie danych osobowych. Dz.U. z 2002 r. nr 101, poz. 926 z późn. zm.).

teleinformatycznych, takie jak adresy IP komputerów czy numery telefonów. Struktura zidentyfikowanych źródła zagrożeń została zaprezentowana na rys. 3.



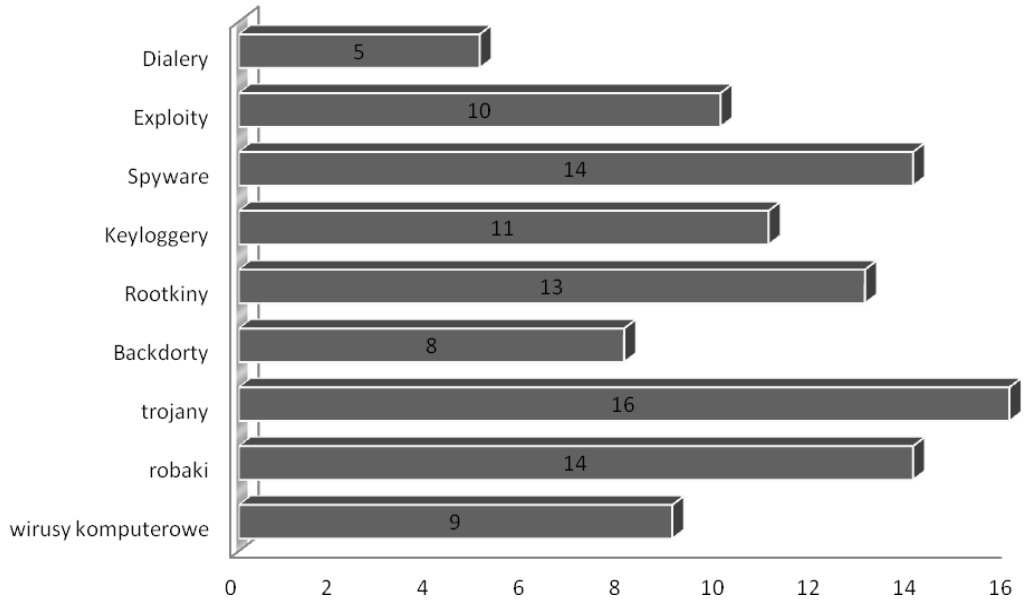
Rys. 3. Struktura źródeł zagrożeń bezpieczeństwa informacji związanych z danymi osobowymi personelu zidentyfikowanych w badanej grupie operatorów usług logistycznych.
Źródło: opracowanie na podstawie badań ankietowych.

Podatność sieci telekomunikacyjnych na zagrożenia dla bezpieczeństwa informacji operatorów usług logistycznych stanowiła kolejne ze zidentyfikowanych źródeł. 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. Strukturę zidentyfikowanych podczas badań źródeł podatności sieci telekomunikacyjnych zaprezentowano na rys. 4. Wyniki przeprowadzonych badań wskazują, iż w prezentowanej grupie dominują zwłaszcza dwa źródła *hotspoty* 37%, oraz bezprzewodowe kanały komunikacyjne 35%, korzystanie z publicznych sieci komunikacyjnych stanowi 21%, zaś jawność danych w czasie transmisji 7% rys. 4.



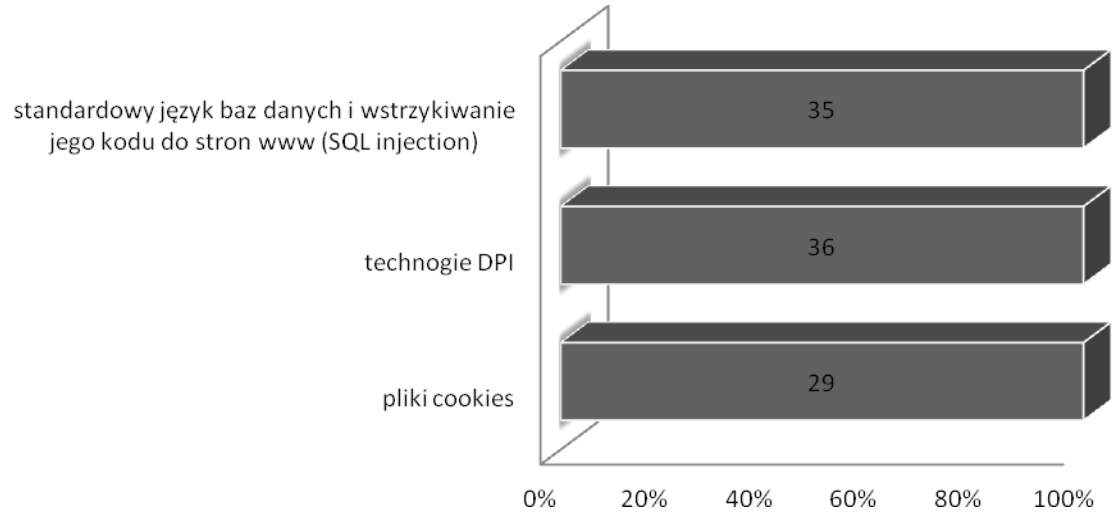
Rys. 4. Struktura źródeł zagrożeń bezpieczeństwa informacji związanych z podatnością sieci teleinformacyjnych zidentyfikowanych w badanej grupie operatorów usług logistycznych.
Źródło: opracowanie na podstawie badań ankietowych.

Istotnym źródłem zagrożeń są również narzędzia programowe wykorzystywane do ataku na bezpieczeństwo informacji operatorów usług logistycznych. Do wspomagania ataku na bezpieczeństwo danych może być użytych wiele różnych metod i narzędzi. Do zidentyfikowanych podczas prowadzonych badań najbardziej znanych i typowych narzędzi wykorzystywanych do działań na szkodę bezpieczeństwa informacji, można zaliczyć narzędzia programowe, takie jak: wirusy komputerowe 9%, robaki 14%, trojany16%, *backdory* 8%, *rootkity 13%*, *keyloggery* programowe 11%, *spyware* 14%, *exploity* 10%, *dialery* 5% – rys. 5.



Rys. 5. Struktura źródeł zagrożeń bezpieczeństwa informacji związanych z narzędziami programowanymi zidentyfikowanymi w badanej grupie operatorów usług logistycznych.
Źródło: opracowanie na podstawie badań ankietowych.

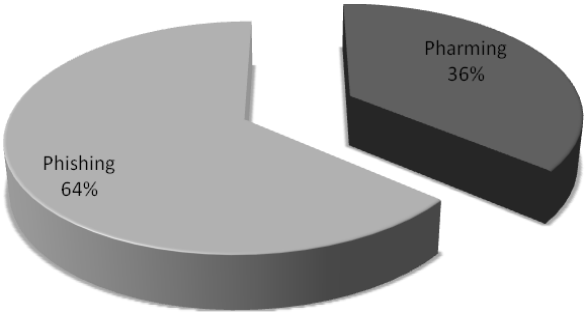
Technologie komputerowe, które mogą być wykorzystywane do kradzieży danych, stanowią kolejne istotne zidentyfikowane źródło zagrożeń dla bezpieczeństwa informacji. Większość narzędzi tworzonych i stosowanych w bezprawnych celach, może być wykorzystywana również dla prowadzenie działań nielegalnych lub 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. Do zidentyfikowanych w tej grupie źródeł zagrożeń można zaliczyć - pliki *cookies* 29%, technologie DPI (ang. *Deep Packet Inspection*) 36%, standardowy język baz danych i wstrzykiwanie jego kodu do stron WWW (*SQL injection*) 35% - rys. 6.



Rys. 6. Struktura źródeł zagrożeń bezpieczeństwa informacji związanych z technologiami komputerowymi zidentyfikowane w badanej grupie operatorów usług logistycznych.
Źródło: opracowanie na podstawie badań ankietowych.

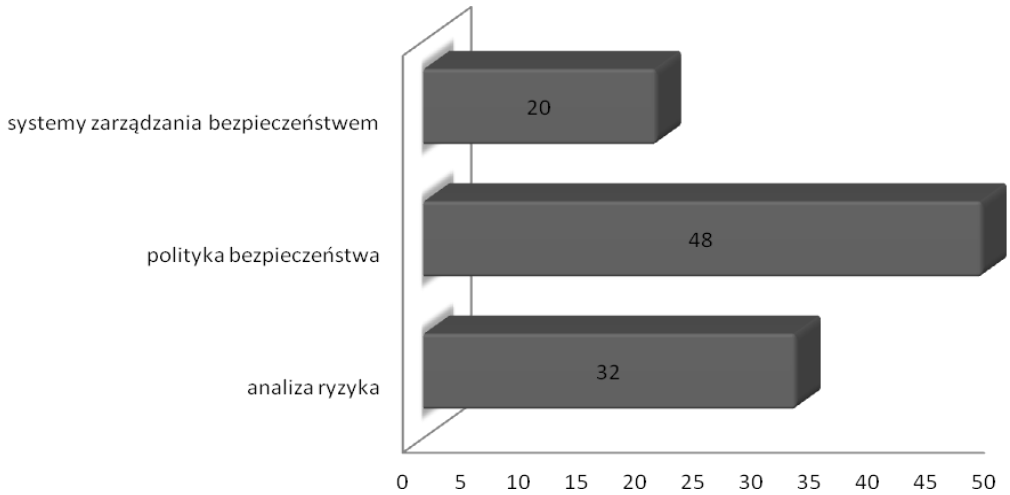
Stosowane socjotechniki w atakach na bezpieczeństwo informacji w sieci, w ramach której funkcjonują operatorzy usług logistycznych stanowiła kolejne ze zidentyfikowanych źródeł zagrożeń. W celu skutecznego zapewnienia bezpieczeństwa informacji przesyłanych między nadawcą i odbiorcą w sieciach teleinformatycznych 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. Warto zaznaczyć, iż w odróżnieniu od źródeł technologii komputerowych, czy też związanych z narzędziami programowanymi technik socjotechniczne, nie wymaga profesjonalnej wiedzy informatycznej i mogą zostać zastosowane właściwie przez każdego. Ponadto płaszczyzny zastosowań są właściwie nieograniczone i wymagają jedynie znajomości samej osoby, na którą kierowany jest atak i jej najbliższego otoczenia. Spośród zidentyfikowanych technik wyróżnić należy *Phishing* oraz *Pharming* – rys. 7. *Phishing* jest jednym z popularniejszych w ostatnim okresie sposobów kradzieży danych, co potwierdzają wyniki badań (64 %), w którym stosowane są elementy tej socjotechniki – która 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 oraz *Pharming* jest specyficzną odmianą *phishingu,* który w badaniu uzyskał 36 % - rys. 7. *Pharming p*olega na modyfikowaniu zawartości serwera nazw domenowych DNS (ang. *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. 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.



Rys. 7. Struktura źródeł zagrożeń bezpieczeństwa informacji związanych z socjotechnikami zidentyfikowane podczas badania grupy operatorów usług logistycznych.
Źródło: opracowanie na podstawie badań ankietowych.

Ostatnim ze zidentyfikowanych źródeł zagrożeń stanowiły obowiązki administratora sieci danych. Systematyczny wzrost zagrożeń dla bezpieczeństwa informacji przetwarzanej przy użyciu systemów teleinformatycznych oraz prawne wymogi ochrony danych operatorów logistycznych sprawiają, że zastosowanie nowoczesnych narzędzi do przetwarzania danych wymaga coraz bardziej profesjonalnego podejścia do bezpieczeństwa informacji. Podejmowane przez administratora danych działania mające na celu zbudowanie systemu bezpieczeństwem informacji i powinny koncentrować się zwłaszcza na trzech zagadnieniach - analizie ryzyka, polityce bezpieczeństwa, systemach zarządzania bezpieczeństwem. Spośród zidentyfikowanych w badaniu zagadnień największe znaczenie zdaniem respondentów związane jest z polityką bezpieczeństwa 48% oraz analizą ryzyka 32% mniejsze znaczenie posiada zarządzanie bezpieczeństwem 20% - rys.8.



Rys. 8. Struktura źródeł zagrożeń bezpieczeństwa informacji związanych z obowiązkami administratora sieci zidentyfikowane w badanej grupie operatorów usług logistycznych.
Źródło: opracowanie na podstawie badań ankietowych.

6. PODSUMOWANIE

Bezpieczeństwo informacji wymaga doskonalenia systemu ochrony, którego celem jest zagwarantowanie możliwie najwyższego poziomu. Obok inwestycji w najnowocześniejsze dostępne na rynku rozwiązania techniczne bardzo ważne są również kwestie organizacyjne oraz świadomość całego personelu. Bezpieczeństwo informacji nie koncentruje się tylko i wyłącznie na zabezpieczeniach informacyjnych czy informatycznych, ale przede wszystkim na odpowiednio przeszkolonych i świadomych pracownikach, jasno określonych zasadach i sposobach postępowania, odpowiednio przygotowanych umowach z klientami, dostawcami i innymi podmiotami, a także sformalizowanych i przetestowanych planach ciągłości działania. Poprowadzone badania ankietowe pozwalają wnioskować, że badani operatorzy usług logistycznych dostrzegają problematykę zagadnienia oraz źródła zagrożenia bezpieczeństwa informacji oraz potrzeb z tym związanych.

Streszczenie

Celem artykułu jest zaprezentowanie wyników badań związanych z bezpieczeństwem informacji wśród operatorów usług logistycznych. Metodyka przeprowadzonych badaniań koncentrowała sie na dwóch aspektach. Pierwszy związany był z dynamiką poziomu potrzeb bezpieczeństwa informacji w łańcuchu dostaw. Drugi dotyczył identyfikacji źródeł zagrożeń mających wpływ na bezpieczeństwo informacji w łańcuchu dostaw, które ujęte zostało przez pryzmat, zagrożeń zewnętrznych związanych z przetwarzaniem bezpieczeństwa informacji, danych osobowych personelu operatora usług logistycznych, podatności sieci telekomunikacyjnych na zagrożenia dla bezpieczeństwa informacji, narzędzi programowych wykorzystywanych do ataku na bezpieczeństwo informacji, technologii komputerowych, które mogą być wykorzystywane do kradzieży danych, stosowanych socjotechnik w atakach na bezpieczeństwo informacji w sieci, oraz obowiązkach administratora sieci danych.

Słowa kluczowe: bezpieczeństwo informacji operatorów usług logistycznych

Security of information as part of the development of supply chains logistics

Abstract

The aim of the article is to present the results of studies relating to the safety of operators information logistics services. Methodology conducted tests have focused on two aspects of the dynamics of the level of security needs in the supply chain and to identify sources of danger in having an impact on the security of information in the supply chain, which was captured by the lens, external threats related to the processing of information security, data logistics service provider staff , telecommunications network vulnerability information security threats, software tools used to attack the security of information, computer technology, which can be used to steal data, used techniques of social engineering attacks on the security of information in the network and data network administrator duties.

Keywords: information security logistics service providers.

LITERATURA

[1] Barczak A., Sydoruk T., *Bezpieczeństwo systemów informatycznych zarządzania*. Warszawa, BELLONA, 2003.
[2] Białas A., *Podstawy bezpieczeństwa systemów teleinformatycznych*. Gliwice, Wydawnictwo: Pracownia komputerowa Jacka Skalmierskiego, 2002.
[3] Cole E., Krutz R. L., Conley J., *Bezpieczeństwo sieci. Biblia*. Warszawa, Helion, 2005.
[4] Kaeo M., *Tworzenie bezpiecznych sieci*. Warszawa, Mikom, 2000.
[5] Kifner T., *Polityka bezpieczeństwa i ochrony informacji*. Gliwice, Helion, 1999.
[6] Kowalewski M., *Aspekty bezpieczeństwa systemów teleinformatycznych*. Warszawa, Instytut Łączności, 2005.
[7] Molski M., Opala S., *Elementarz bezpieczeństwa systemów informatycznych*. Warszawa, Mikom, 2002
[8] Ustawa z dnia 29 sierpnia 2997 r. o ochronie danych osobowych. Dz.U. z 2002 r. nr 101, poz. 926 z późn. zm.).