Zeszyty Naukowe No 2(7) 2017
Quality. Production. Improvement s. 12-19

Justyna Żywiołek[1]

BEZPIECZEŃSTWO INFORMACYJNE W ŁAŃCUCHU DOSTAW WYBRANE ZAGADNIENIA

Streszczenie: Współcześnie funkcjonujące przedsiębiorstwa zmuszone są do działania na rynku globalnym, wynikiem czego jest uczestniczenie w łańcuchach lub sieciach dostaw. Niezbędnym elementem istnienia przedsiębiorstwa są przepływy w łańcuchu. Konsekwencją jest wymuszone współdzielenie informacji. Można zatem stwierdzić, iż przedsiębiorstwo nie może istnieć na rynku samodzielnie. Warunki zauważalne na globalnym rynku w ostatnich latach wskazują na potrzebę tworzenia i wdrażania narzędzi podnoszących poziom bezpieczeństwa łańcucha dostaw. Artykuł przedstawia problematykę zapewnienia bezpieczeństwa przepływu informacji w łańcuchu dostaw.

Słowa kluczowe: łańcuch dostaw, przepływy informacyjne, obieg informacji, bezpieczeństwo w łańcuch dostaw

1. Wstęp

Na przestrzeni ostatni lat można zaobserwować potrzebę ochrony przedsiębiorstw przed możliwością wystąpienia różnorodnych sytuacji niepożądanych w łańcuchach dostaw. Ta tendencja jest szczególnie zauważalna w łańcuchach międzynarodowych. Łańcuchy dostaw są bardzo rozbudowane, a tym samym coraz bardziej podatne na zdarzenia negatywne, nie tylko o charakterze przypadkowym, ale i celowym. Łańcuch ten jest atrakcyjnym adresatem takich działań, wśród których są tak poważne, jak ataki terrorystyczne, kradzież czy przemyt towaru. Tu szczególnie dotkliwe starty odnoszą takie branże, jak: elektroniczna, metalowa, odzieżowa, tytoniowa i rolno-spożywcza.

Zjawisku rosnącego zagrożenia atakiem na łańcuch dostaw sprzyja niewątpliwie globalizacja handlu, rozdrobnione i szerokie sieci dostawców, kooperantów, w tym konieczność oszczędności kosztów związana z korzystaniem z takich usprawnień, jak outsourcing i offshoring, które zwiększają, a nie redukują ryzyko utraty kontroli nad produktem i jego bezpieczeństwem w procesie logistycznym.

2. Pojęcie łańcucha dostaw

W literaturze można znaleźć wiele definicji łańcucha dostaw. Definiując to pojęcie autorzy, wskazują bowiem na różne aspekty, istotne w funkcjonowaniu tego łańcucha.

[1] Dr inż., Politechnika Częstochowska, Wydział Zarządzania, Katedra Inżynierii Produkcji i Bezpieczeństwa, e-mail: justyna.zywiolek@wz.pcz.pl

B. Bozarth i R.B. Handfield definiują łańcuch dostaw jako sieć producentów i usługodawców, którzy prowadzą współpracę od pozyskiwania surowca do zakupu przez użytkownika końcowego. Zwracają oni szczególną uwagę na to, że wszystkie etapy połączone są ze sobą przepływami dóbr fizycznych, przepływami informacji oraz przepływami pieniężnymi (Bozarth, HANDFIELD 2007). M. Christopher dostrzega, że łańcuch dostaw to sieć organizacji, powiązanych poprzez z dostawcami i odbiorcami, w różne procesy i działania, które tworzą wartość w postaci produktów i usług Christopher 1998].Natomiast P.K Bagchi, zakłada że łańcuch ten składa się z zakładów i wykonawców, którzy dostarczają surowców i komponentów, następnie przerabiają je w półprodukty, potem produkują z nich produkty finalne (GROTTEl, 2013). Łańcuch dostaw traktowany jest również często jako struktura lub grupa przedsiębiorstw realizująca wspólne działania służące zaspokojeniu popytu na określone produkty (FERTSCH (red.) 2006).

Definiując łańcuch dostaw należy podkreślić także, iż istotny jest również towarzyszący wszystkim tym procesom przepływ informacji od samego powstania produktu aż do znalezienia się dobra u finalnego odbiorcy.Autorzy nie biorąc pod uwagę charakteru łańcucha i sposobu podejścia, zawsze podkreślają dominującą rolę klienta i konieczność przepływu informacyjnego (MAJDECKI, 2013). M. Christopher uważa, należy dążyć do sytuacji gdy klient ma wiedzę o produkcie, jest przekonany o jego wysokiej jakości, niezawodności, ma dostęp do odpowiedniego wsparcia technicznego i wyposażony jest we wszelakie niezbędne mu informacje (CHRISTOPHER 1998).

3. Bezpieczeństwo łańcucha dostaw

Bezpieczeństwo to termin, który używany jest w wielu różnych dziedzinach. Można je rozpatrywać w kategorii jednostki, grupy czy narodu w kontekście społeczności oraz w kategoriach bezpieczeństwa fizycznego i informatycznego w kontekście przedsiębiorstw (BIAŁAS, 2007).

Należy podkreślić, iż zapewnienie bezpieczeństwa każdemu użytkownikowi systemu informacyjnego i informatycznego powinno być jednym z priorytetów (ŻYWIOŁEK, 2015). Każde przedsiębiorstwo próbuje jak najlepiej zabezpieczyć swoje dane i informacje (ŻYWIOŁEK, 2012). W celu poprawy bezpieczeństwa informatycznego należy zastosować wszystkie istniejące środki bezpieczeństwa, przeszkolić personel w zakresie ich odpowiedniego użytkowania, a także zadbać o bezpieczeństwo danych przechowywanych w systemach teleinformatycznych przy użyciu odpowiednich programów zabezpieczających (ŻYWIOŁEK, STANIEWSKA, 2012).

Bezpieczeństwo w łańcuchu dostaw może być rozumiane jako stan, zbiór procesów i procedur, czyli środków ochrony, pozwalających na utrzymanie ciągłego

przepływu dóbr od miejsca ich powstania do końcowego nabywcy, bez przestojów i zakłóceń, zarówno w obrębie łańcucha dostaw, jak i w jego otoczeniu (ŻYWIOŁEK, 2015). Należy podkreślić iż zagadnienia bezpieczeństwa nie dotyczą tylko fizycznej kradzieży, ale związane jest z naruszeniem własności intelektualnej, cyberterroryzmem, szpiegostwem gospodarczym, a także wykorzystywaniem systemów obsługi łańcuchów dostaw do przestępstw takich jak przewóz nielegalny, przemyt ładunków lub ludzi (WITKOWSKI, 2010).

Mimo że ataki cyberterroryzmu w łańcuchu dostaw wydają się być mało to zdarzenia, takie jak kradzież danych to zagrożenie uznawane za najbardziej możliwe, a jego wystąpienie ze względu na jego skutki i zasięg może mieć ogromne konsekwencje dla przedsiębiorstw (WIETESKA G., 2011).

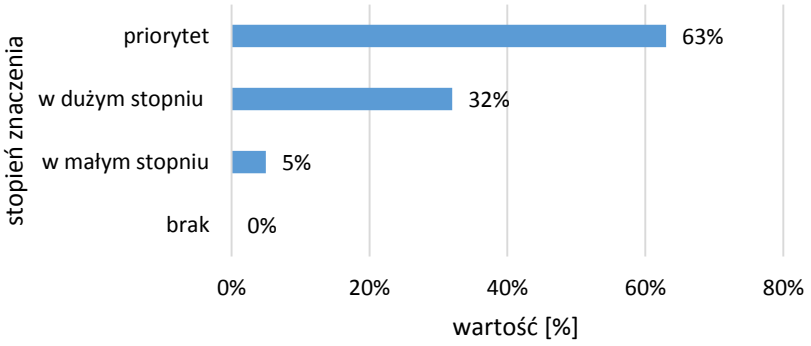
4. Bezpieczeństwo informacji w łańcuchu dostaw

Artykuł przedstawia wyniki badań dotyczące bezpieczeństwa informacyjnego w łańcuchach dostaw. Podstawą badań była ankieta skierowana do 83 przedstawicieli różnych podmiotów w zakresie bezpieczeństwa informacyjnego w łańcuchu dostaw. Ponad dwie trzecie badanych osób reprezentowało duże podmioty, zatrudniające powyżej 250 pracowników. Zdecydowana większość ankietowanych to informatycylub pełnomocnicy zarządu ds. bezpieczeństwa. Celem badania była identyfikacja wartości informacji w łańcuchu dostaw i roli bezpieczeństwa w łańcuchu dostaw.

Pierwsze z badanych zagadnień dotyczyło świadomości pracowników przedsiębiorstw w zakresie wartości, jaką reprezentują informacje. Strukturę otrzymanych wskazań na pytanie „w jakim stopniu przywiązuje się wagę do znaczenia informacji oraz jej bezpieczeństwa?” przedstawia rysunek 1.

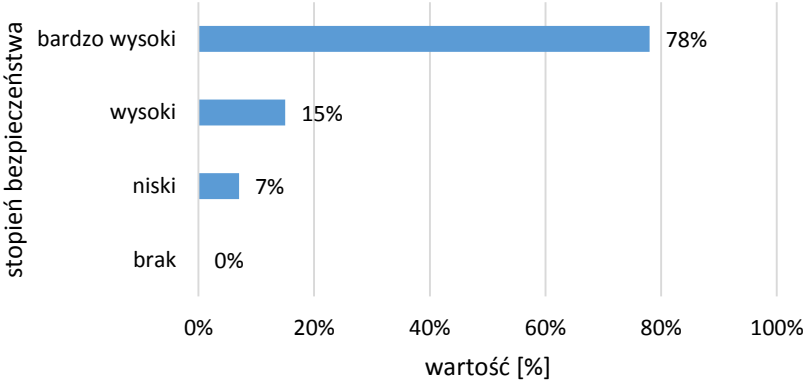
O wysokim poziomie świadomości na temat wartości informacji świadczy 53% ankietowanych uznających bezpieczeństwo informacji, jako jeden z priorytetów organizacji. Nikt z ankietowanych nie stwierdził, że informacja w ogóle nie ma znaczenia, a jej ochrona w ogóle nie jest brana pod uwagę. Pomimo problemów z dokładnym oszacowaniem wartości informacji przepływających pomiędzy przedsiębiorstwami współpracujących w łańcuchach dostaw, respondenci zdają sobie sprawę z dużej ich wagi, w szczególności tych stanowiących tajemnice przedsiębiorstwa, stąd tak duży nacisk na ich ochronę.

Z przeprowadzonego badania wynika, że organizacje mają świadomość z dużej wartości informacji, a jej bezpieczeństwo uważa się za jeden z priorytetów (rys. 2).



Rys. 1. Znaczenie informacji w przedsiębiorstwie

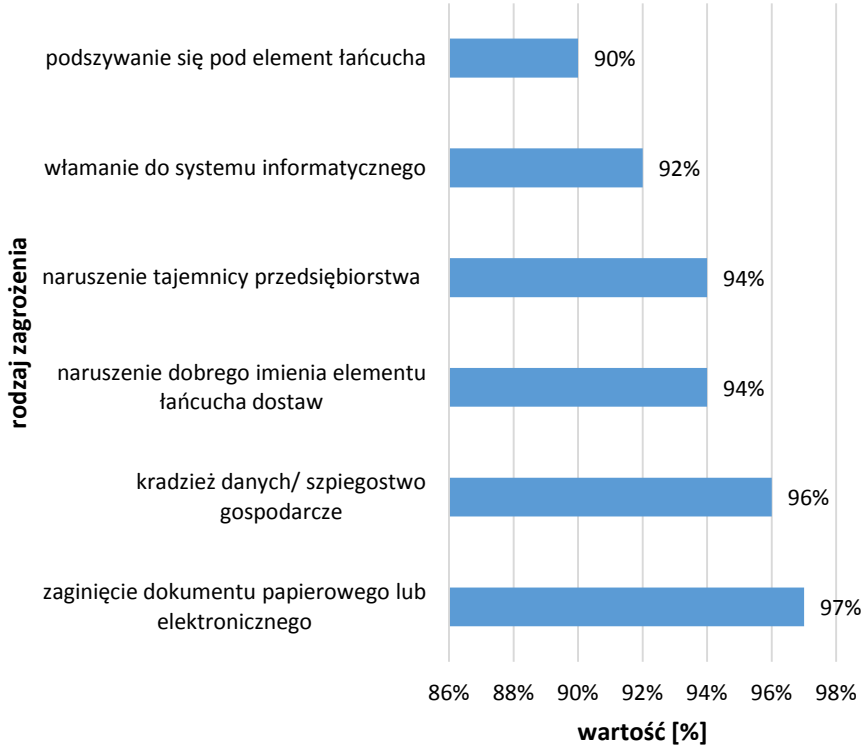
Źródło: Opracowanie własne na podstawie badań



Rys. 2. Bezpieczeństwo przepływów informacyjnychw łańcuchu dostaw

Źródło: Opracowanie własne na podstawie badań

Wraz ze wzrostem świadomości w zakresie przepływów informacyjnych w łańcuchu dostaw, bezpieczeństwa informacji, wzrasta również świadomość konieczności zabezpieczania przepływów w łańcuchu dostaw. Wyniki badania dotyczące zagrożeń przepływów informacyjnych w łańcuchu dostaw przedstawia rysunek 3.



Rys. 3. Zagrożenia bezpieczeństwa informacyjnego w łańcuchu dostaw

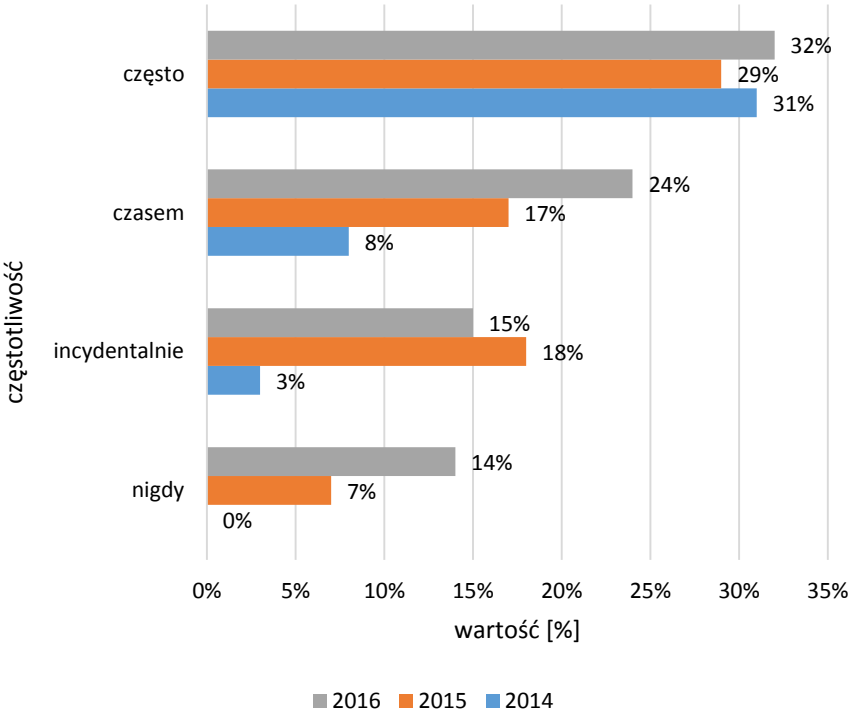
Źródło: Opracowanie własne na podstawie badań

Otrzymane wyniki badań wskazują na różnorodność możliwych zagrożeń w zakresie bezpieczeństwa informacji w łańcuchu dostaw. Biorąc pod uwagę motywacje, jakimi kierują się przestępcy czy sprawcy wystąpienia incydentu, najwięcej badanych wskazało jako zagrożenie zaginięcie dokumentu papierowego lub elektronicznego, co z całą pewnością następuje stanowiąc incydent wycieku informacji. Istotnym czynnikiem była również możliwość kradzieży danych lub szpiegostwa gospodarczego.

Z danych badanych przedsiębiorstw wynika również, iż nie są one tylko narażone na wystąpienie zagrożenia. Incydenty występujące w badanych przedsiębiorstwach zdaniem ankietowanych, przedstawia rysunek 4.

Ankietowani dostrzegają problem występowania incydentów bezpieczeństwa informacyjnego w łańcuchu dostaw. Zróżnicowanie odpowiedzi świadczy o tym, iż w badanych przedsiębiorstwach świadomość pracowników jest na różnym poziomie. Brak wiedzy na ten zagrożeń jest powodem występowania incydentów.

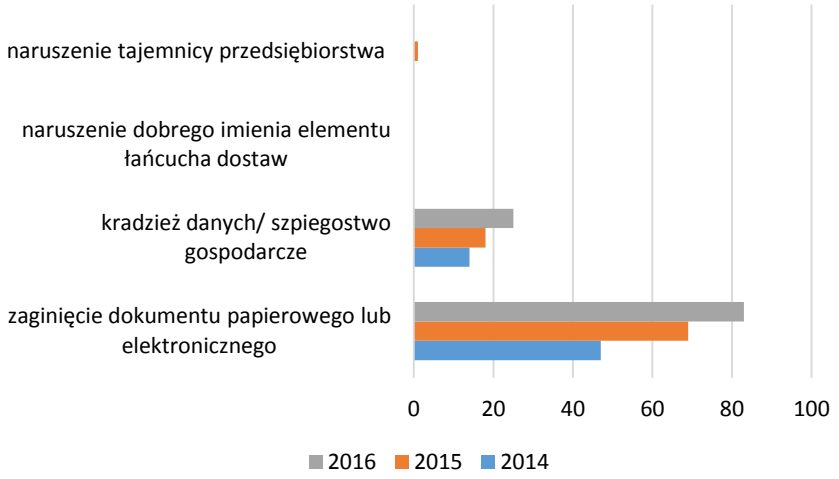
Realnie występujące zagrożenia które miały miejsce w badanych przedsiębiorstwach przedstawia rysunek 5.



Rys. 4. Występowanie incydentów bezpieczeństwa informacyjnego w łańcuchu dostaw zdaniem ankietowanych

Źródło: Opracowanie własne na podstawie badań

Najczęściej występującym incydentem jest zaginięcie dokumentu. Z roku na rok ginie coraz więcej dokumentów elektronicznych. Pracownikom przedsiębiorstw wydaje się, że to oni usunęli dany plik lub mail, nie dostrzegają możliwości włamania na ich pocztę mailową lub komputer. Incydentalnym wydarzeniem było naruszenie tajemnicy przedsiębiorstwa. Wynikało to z działań byłego pracownika jednej z firm. Działał on na szkodę byłego pracodawcy. Wobec niego zostały wyciągnięte konsekwencje prawne. W badanych przedsiębiorstwach w badanym okresie nie miały miejsca naruszenia dobrego imienia elementu łańcucha dostaw.



Rys. 5. Występowanie incydentów bezpieczeństwa informacyjnego w łańcuchu dostaw w latach 2014-216

Źródło: Opracowanie własne na podstawie badań

5. Podsumowanie

Zagrożenia związane z bezpieczeństwem informacyjnym są zjawiskiem stosunkowo nieznanym i nowym. Tego rodzaju działania mogą występować w każdego rodzaju i wielkości przedsiębiorstwie.

Wyniki przedstawionych badań ankietowych wskazują, że w badanych przedsiębiorstwach przywiązuje się istotną wagę do kwestii związanych z bezpieczeństwem informacyjnym w łańcuchu dostaw. Wiele ankietowanych osób wskazało jako jeden z priorytetów działalności przepływ informacji i jej bezpieczeństwo.

W przedsiębiorstwach mogą mieć miejsce zdarzenia negatywne przekładające się na utratę dobrego wizerunku lub prowadzące do zaprzestania współpracy handlowej. Badania ankietowe pozwoliły na identyfikację możliwych zagrożeń oraz realnych incydentów występujących w przedsiębiorstwach, co stanowi podstawę do dalszych badań w tym zakresie.

Bibliografia

1. BOZARTH C. B., HANDFIELD R. B., 2007, *Wprowadzenie do zarządzania operacjami i łańcuchem dostaw*, Helion, Gliwice.

2. CHRISTOPHER M.,1998, Logistics and supply chain management: Strategies for reducing costs and im-proving service, Financial Times – Prentice Hall, LONDON.FERTSCH M. (red.), 2006, Słownikterminologiilogistycznej, ILiM, Poznań.
3. GROTTEL M., 2013, *Instytucja upoważnionego przedsiębiorcy – nowa jakość obsługi celnej podmiotów gospodarczych*, „Biznes Międzynarodowy w Gospodarce Globalnej", nr 32, s. 97-113, http://ec.europa.eu/taxation_customs/dds2/eos/aeo_consultation.jsp?Lang=pl (15.04.2014).
4. PIRES S. R. I., BREMER C. F., DE SANTA EULALIA L. A., GOULART C. P., 2001, *Supply chain and virtual enterprise: Comparison, migration and a case study*, „International Journal of Logistics: Research and Application", nr 4(3), s. 297-311.
5. WIETESKA G., 2011, *Bezpieczeństwo w sieci dostaw*, Acta Universitatis Lodziensis, Folia Oeconomica, nr 258, s. 149-162.
6. WITKOWSKI J., 2010, *Zarządzanie łańcuchem dostaw*, PWE, Warszawa.
7. CIBOROWSKI L., *Zarządzanie i informacja w obliczu wyzwań współczesności,* [w:] *Przedsiębiorstwo wobec współczesnych wyzwań w procesie zarządzania,* (red.) Hejduk I., Ciborowski L., Wyd. Akademii Podlaskiej, Siedlce, 2005, s. 24.
8. BIAŁAS A., *Bezpieczeństwo informacji i usług w nowoczesnej firmie*, WNT, Warszawa, 2007.
9. KLONOWSKI Z., *Systemy informacyjne zarządzania przedsiębiorstwem. Modele rozwoju i własności funkcjonalne*, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław, 2004.
10. MAJDECKI M., *Zarządzanie bezpieczeństwem informacji*, Forum Jakości nr 1/2005.
11. ŻYWIOŁEK J., STANIEWSKA E., *Zagrożenia zarządzania bezpieczeństwem informacji w przedsiębiorstwi*e, Logistyka nr 6, 2012.
12. ŻYWIOŁEK J., *Wpływ obniżania jakości informacji na przepływ informacji w przedsiębiorstwie*, Logistyka nr 6, 2012.
13. ŻYWIOŁEK J., *Innowacyjność przepływów informacyjnych jako element udoskonalenia systemu informacji w przedsiębiorstwie logistycznym*, Zeszyty Naukowe Politechniki Częstochowskiej. Zarządzanie, s. 63-71, 2015.
14. ŻYWIOŁEK J., *Technologie monitorowania zagrożeń bezpieczeństwa w przedsiębiorstwach,* Światowy Dzień Bezpieczeństwa i Ochrony Zdrowia w Pracy. Kształtowanie bezpieczeństwa pracy (red.) Roman Magdalena, Wydawnictwo Wydziału Zarządzania Politechniki Częstochowskiej, 2015, s. 101-110.