ACTA UNIVERSITATIS LODZIENSIS
FOLIA OECONOMICA 258, 2011

*Grażyna Wieteska**

BEZPIECZEŃSTWO W SIECI DOSTAW

1. WSTĘP

Obserwowane w ostatnich latach skutki zakłóceń rozchodzące się wzdłuż łańcuchów dostaw świadczą o potrzebie zwrócenia uwagi na konieczność implementacji przez przedsiębiorstwa narzędzi, które determinują zapobieganie występowaniu zdarzeniom niepożądanym i w związku z tym skuteczne prowadzenie działań w turbulentnym otoczeniu. Coraz większego znaczenia nabiera problematyka podatności ogniw na zdarzenia losowe[1], w tym zamierzone działania człowieka mające na celu spowodowanie zniszczeń i strat. Jest ona szczególnie ważna w międzynarodowych łańcuchach dostaw. W poszukiwaniu obniżki kosztów przedsiębiorstwa chętnie stosują outsourcing, a także w ramach strategii LCCS (ang. *Low Cost Country Sourcing*) offshoring polegający na przenoszeniu własnej działalności lub oddawaniu procesów w outsourcing – poza granice kraju, zwłaszcza do Azji, Ameryki Południowej i Środkowo-wschodniej Europy[2]. Tym samym powstają globalne łańcuchy dostaw i zwiększa się stopień skomplikowania powiązań gospodarczych. W efekcie obserwuje się wzrost poziomu ryzyka dla procesów przepływu surowców, materiałów, wyrobów gotowych oraz informacji. Celem artykułu jest zwrócenie uwagi na zagadnienie, jakim jest bezpieczeństwo sieci dostaw oraz zaprezentowanie dobrych praktyk, inicjatyw i koncepcji powstających w tym obszarze.

* Doktor, adiunkt, Katedra Zarządzania Jakością, Wydział Zarządzania, Uniwersytet Łódzki.

[1] Zdarzenie losowe to zdarzenie przyszłe i niepewne, powodujące uszczerbek w dobrach osobistych lub majątkowych, niezależne od woli człowieka i następujące wbrew jego woli. Ustawa o działalności ubezpieczeniowej Dz. U. 2010.11.66.

[2] Państwa najbardziej atrakcyjne z punktu widzenia offshoringu to: Indie, Chiny, Malezja, Tajlandia, Indonezja, kraje Ameryki Południowej (Brazylia, Chile) oraz Europy (Estonia, Litwa, Czechy, Polska). Raport A.T. Kearney pt. *Geography of Offshoring is Shifting*, 2009 r. Oszczędności wynikają z niższych kosztów pracy, mniej restrykcyjnych przepisów prawnych z zakresu bhp i ochrony środowiska, tańszych materiałów, niższych podatków. J. Leonard, *How Structural Costs Imposed on U.S. Manufacturers Harm Workers and Threaten Competitiveness*, Raport National Association of Manufacturers, December 2003.

2. PROBLEMATYKA BEZPIECZEŃSTWA

Przedstawienie problematyki bezpieczeństwa należy rozpocząć od wyjaśnienia pojęcia bezpieczeństwa. Termin ten jest powszechnie stosowany w praktyce gospodarczej, definiuje się go też w wielu naukach[3]. Bezpieczeństwo rozumiane jest najczęściej jako stan, w którym większość zagrożeń zostało zidentyfikowanych, a ryzyko potencjalnych zdarzeń niepożądanych oszacowano, ograniczono i zaakceptowano. Z punktu widzenia łańcucha dostaw wyróżnić można bezpieczeństwo wewnętrzne, będące efektem niezawodnych i stabilnych procesów w jego ogniwach, oraz zewnętrzne, oznaczające brak znaczącego ryzyka ze strony źródeł antropogenicznych i naturalnych[4]. W warunkach zagrożeń o charakterze międzynarodowym (np. terroryzm, przemyt) bezpieczeństwo definiowane jest jako fizyczna ochrona infrastruktury technicznej przedsiębiorstwa, ładunku w transporcie oraz informacji z nim związanej. Przedmiotem bezpieczeństwa stają się w związku z tym systemy informatyczne, porty, magazyny, terminale, personel, ładunki i środki transportu[5].

Problematyka bezpieczeństwa wiąże się z zagadnieniem ciągłości działania, co w przypadku łańcucha dostaw rozumieć należy jako utrzymanie sprawności i stabilności realizowanych w nim procesów: zaopatrzenia, produkcji, magazynowania i transportu dostaw oraz przepływu informacji. Zapewnić to mają działania prewencyjne oraz utworzone procedury awaryjne (plany ciągłości), przygotowywane na wypadek wystąpienia drobnych incydentów, a także sytuacji kryzysowych, których niebezpieczeństwo tkwi w nieprzewidywalności i braku całkowitej kontroli nad rozwojem przyszłych scenariuszy zdarzeń. W ten sposób przedsiębiorstwa dążą do wykształcenia zdolności, która oznacza, że nawet w sytuacji poważnego zakłócenia, poprzez odpowiednie sterowanie ryzykiem w celu jego złagodzenia, poziom obsługi klienta utrzymany zostanie na zakładanym poziomie.

Jak pokazują wyniki badań, wiele firm odczuwa skutki fizycznych zniszczeń pojawiających się w ich łańcuchach dostaw. Wśród najważniejszych przyczyn tych strat wymienia się: działania celowe człowieka (m.in. ataki terrorystyczne, przemyt, kradzieże), katastrofy naturalne, awarie infrastruktury technicznej, pożary, eksplozje, wypadki komunikacyjne[6]. Historia dostarcza wielu przykładów kryzysów pojawiających się w łańcuchach dostaw. Przykła-

---

[3] Por. Z. Nowak, *Zarządzanie środowiskiem*, cz. 2, Wyd. Politechniki Śląskiej, Gliwice 2001, s. 309–310.

[4] Por. R. Zięba, *Kategorie bezpieczeństwa w nauce o stosunkach międzynarodowych*, [w:] D.B. Bobrow, E. Haliżak, R. Zięba (red.), *Bezpieczeństwo narodowe i międzynarodowe u schyłku XX w.*, Wydawnictwo Naukowe Scholar, Warszawa 1997, s. 4.

[5] I. Manuj, J.T. Mentzer, *Global Supply Chain Risk Management*, "Journal of Business Logistics", Vol. 29, No. 1, 2008, s. 133–153; R. Sarathy, *Security and the Global Supply Chain*, "Transportation Journal", Vol. 45, No. 4, 2006, s. 28–52.

[6] *Physical Risks to the Supply Chain*, CFO Publishing Corp., February 2009.

dami poważnych zakłóceń, które wystąpiły w ciągu ostatnich lat są: eksplozja platformy wiertniczej i długotrwały wyciek paliwa do wód Zatoki Meksykańskiej, awaria w zakładach na Węgrzech, gdzie ze zbiornika wydostała się do pobliskich rzek i miast ogromna ilość toksycznych substancji, powodzie w Europie i Australii, problemy z zapewnieniem stabilności reaktorów w elektrowniach atomowych po trzęsieniu ziemi w Japonii, cyberterrorystyczny atak na jedną z firm, dostarczającą usługi dla użytkowników konsol i miłośników gier w sieci czy epidemia spowodowana pojawieniem się w Europie w sprzedaży kiełków fasoli z groźnymi bakteriami E. Coli. Tego typu zdarzenia wpływają nie tylko na pojedyncze łańcuchy dostaw, ale mogą powodować destabilizację globalnej gospodarki, o czym w niektórych przypadkach świadczą drastyczne reakcje światowych giełd[7]. Warto więc zauważyć, iż jednym z ważniejszych elementów skutecznego funkcjonowania dzisiejszych sieci dostaw jest zapewnienie ich bezpieczeństwa. Między innymi dlatego obserwuje się wzrost zainteresowania omawianą problematyką zarówno na szczeblu rządowym, jak i w sektorze prywatnym.

3. OCENA RYZYKA JAKO FUNDAMENT DLA BUDOWANIA BEZPIECZEŃSTWA W ŁAŃCUCHU DOSTAW

Budowanie bezpieczeństwa procesów przepływu w przedsiębiorstwie oraz w relacjach z dostawcami i klientami powinno rozpocząć się od analizy, która dostarczy informacji na temat aktualnego poziomu ryzyka, wskaże najbardziej podatne na zakłócenia miejsca w łańcuchu dostaw, a także pozwoli rozpoznać obecne i potencjalne zagrożenia dla bezpieczeństwa procesów przepływu. Uporządkowanie wiedzy na ten temat warunkowane jest przeprowadzeniem dokładnej oceny ryzyka, która obejmuje kilka następujących etapów:

- zidentyfikowanie zagrożeń i rodzajów zdarzeń niepożądanych (scenariuszy zdarzeń), które mogą się zrealizować oraz przyczyn źródłowych (*rootcause*) określonych zakłóceń, stosując np. metodę FTA (*Failure Tree Analysis*);
- rozpoznanie podatności na zakłócenia (*vulnerability*) i pomiar ryzyka poprzez określenie prawdopodobieństwa realizacji zdarzenia oraz wielkości jego skutków (np. w ich odniesieniu do wartości aktywów, zdolności prowadzenia procesów kluczowych firmy, liczby ofiar śmiertelnych, wpływu na reputację), a także w niektórych przypadkach czasu ekspozycji na za-

[7] Wiele firm odczuwa straty na skutek silnych zmian w makrootoczeniu, w tym m.in. przedsiębiorstwa świadczące usługi logistyczne (*third-party logistics*). G. Bisignani, generalny dyrektor IATA, oświadczył dn. 6 czerwca 2011 r. na 67 generalnym spotkaniu Międzynarodowego Zrzeszenia Przewoźników Powietrznych, że branża lotnicza notuje straty, których przyczynami są wzrost kosztów paliwa, zamieszki polityczne, a także katastrofy naturalne, w tym trzęsienie ziemi i tsunami w Japonii, www.iata.org/events/agm/2011/gallery/Pages/video-gallery.aspx?vid=7 dn. 6 czerwca 2011 r.

kłócenia (np. analizując ryzyko zawodowe, sytuacje kryzysowe przy wykorzystaniu metody *Risk Score*) czy zdolność do skutecznej detekcji błędu w procesie/wady w wyrobie (np. stosując metodę FMEA – *Failure Mode and Effects Analysis*);

- ewaluacja ryzyka zdarzeń, czyli określenie akceptowalności ryzyka (np. przy zastosowaniu metody ALARP – *As Low As Reasonably Practicable*);
- wskazanie priorytetowych obszarów dla działań zwiększających bezpieczeństwo.

Ocena ryzyka wymaga dużej ilości informacji, która determinuje, zwłaszcza w warunkach niepewności[8], dokładność analiz (tab. 1). Każda zmiana w zewnętrznym i wewnętrznym otoczeniu jednostki gospodarczej może być przyczyną obniżenia poziomu bezpieczeństwa w łańcuchu dostaw. Dlatego ocena ryzyka powinna być przeprowadzana regularnie celem aktualizowania wiedzy o zagrożeniach i poziomie bieżącego ryzyka.

Tabela 1

Informacja niezbędna do przeprowadzenia oceny ryzyka

Źródła informacji niezbędnej do przeprowadzenia oceny ryzyka	Opis źródła informacji	Rodzaj informacji
Pracownicy przedsiębiorstwa, eksperci	Najwyższe kierownictwo, personel zatrudniony na poziomie taktycznym i operacyjnym, eksperci z zewnątrz.	Zaobserwowane problemy podczas wykonywania pracy i pomysły na ich wyeliminowanie, dobre praktyki, wiedza płynąca z doświadczenia.
Bazy danych	Wewnętrzne bazy danych firmy zawierające informacje na temat zakłóceń, które miały miejsce w ostatnich latach; zewnętrzne bazy danych: raporty Głównego Urzędu Statystycznego, Państwowej Inspekcji Pracy, Wojewódzkich Inspektoratów Ochrony Środowiska, Komendy Głównej Policji.	Informacje o częstości występowania zdarzeń niepożądanych, zmianach w firmie i makrootoczeniu, trendach.
Wymagania	Przepisy prawne (np. z zakresu bhp, ochrony środowiska), wymagania standardów technicznych, wymagania systemów zarządzania, wymagania klientów, wewnętrzne regulacje firmy, polityki przedsiębiorstw.	Dopuszczalne wartości parametrów procesów i wyrobów, konkretne specyfikacje, praktyczne rozwiązania techniczne i technologiczne, najlepsze praktyki.

Źródło: opracowanie własne.

[8] Niepewność to „niezdolność do przewidzenia dokładnego prawdopodobieństwa lub efektów przyszłych zdarzeń". *Enterprise Risk Management Framework*, COSO 2004, s. 15.

Głównym źródłem informacji na temat ryzyka w przedsiębiorstwie są pracownicy, zwłaszcza operacyjni. Posiadają oni wiedzę o zaobserwowanych podczas codziennie wykonywanej pracy problemach i często także pomysły na zwiększenie bezpieczeństwa. Najwyższe kierownictwo ocenić może natomiast wpływ zmian makroekonomicznych oraz ryzyka operacyjnego na cele strategiczne firmy. Eksperci dysponują z kolei wiedzą na temat dobrych praktyk czy niedostrzeżonych dotąd przez firmę zagrożeń. Bazy danych (zewnętrzne i wewnętrzne) pozwalają na ocenę częstości występowania określonych zdarzeń w firmie bądź w skali, np. całego kraju. Wymogi, które firma musi spełnić (np. przepisy prawne), lub które dobrowolnie zaimplementowała (np. wymagania norm), a także inne, jak wymagania klientów, stanowią informację niezbędną do zidentyfikowania zagrożeń i przeprowadzenia racjonalnej akceptacji ryzyka.

4. BUDOWANIE BEZPIECZEŃSTWA PROCESÓW PRZEPŁYWU TOWARU I INFORMACJI W ŁAŃCUCHU DOSTAW

W ostatnich latach powstała koncepcja zarządzania bezpieczeństwem łańcucha dostaw (*Supply Chain Security Management*, SCSM), która ujmuje bezpieczeństwo jako ochronę (*security*) aktywów łańcucha dostaw, w tym relacji gospodarczych, wydajności i skuteczności[9]. Podejście to opiera się na współpracy przedsiębiorstw z partnerami gospodarczymi, jednostkami publicznymi i rządem, a także konkurencją[10] w zakresie utworzenia polityk, procedur i planów działań oraz zapewnienia technologii służącej ochronie aktywów łańcucha dostaw, m.in. przed kradzieżami, terroryzmem czy bezprawnym przemytem ludzi i broni masowego rażenia[11]. Wśród głównych przyczyn zainteresowania przedsiębiorstw zwiększaniem bezpieczeństwa procesów przepływu dostaw i informacji wymienić należy ochronę marki (w tym chęć zapobiegania nielegalnej sprzedaży, zagwarantowania klientom oryginalnego, bezpiecznego produktu), wymagania klientów z tego zakresu oraz obowiązujące przepisy prawne[12]. Z kolei wśród korzyści związanych z implementacją koncepcji zarządzania bezpieczeństwem łańcucha dostaw firmy wskazują wzrost bezpieczeństwa ładunków (redukcja liczby kradzieży i przypadków zmian jakości technicznej ładunków), zwiększenie przeźroczystości łańcucha dostaw (wzrost dostępności do danych, np. informacji na temat miejsca, w którym

[9] Z. William, J.E. Leug, S.A. LeMay, *Supply Chain Security: An Overview and Research Agenda*, "International Journal of Logistics Management", Vol. 19, No. 2, 2008, s. 254–258.

[10] Tamże.

[11] D.J. Closs, E.F. McGarrell, *Enhancing Security throughout the Supply Chain*, Special Report Series, IBM Center for the Business Government, April 2004, s. 8.

[12] D. Closs, C. Speier, J. Whipple, A.M. Voss, *Framework for Protecting Your Supply Chain*, "Supply Chain Management Review", Vol. 12, No. 2, 2008, s. 38–45.

znajduje się ładunek), redukcję czasu transportu, sprawniejsze manipulowanie towarem (w wyniku m.in. automatyzacji procesów), skuteczniejszą odprawę celną (np. redukcja liczby kontroli na granicach celnych), a także wzrost satysfakcji nabywcy i mniej reklamacji[13].

Koncepcja SCSM szczególnie koncentruje się na zapewnianiu fizycznego bezpieczeństwa ładunków oraz kontroli infrastruktury technicznej, systemów informatycznych, zasobów ludzkich oraz dostaw. Wśród dobrych praktyk TPAT (*Customs-Trade Partnership against Terrorism*) z tego zakresu znajdują się:

- wymagania wobec partnerów gospodarczych (*business partner requirements*),
- udział w inicjatywach rządowych, certyfikacja (*program membership/certifications*),
- kontrola dostępu (*physical access control*),
- bezpieczeństwo personelu (*personnel security*),
- ochrona fizyczna (*physical security*),
- szkolenia (*security training*, *threat awareness*, *outreach*),
- zabezpieczenia proceduralne (*procedural security*),
- bezpieczeństwo informatyczne (*Information Technology security*),
- gotowość na sytuacje awaryjne, odzyskiwanie danych w sytuacji kryzysu (*emergency preparedness/disaster recovery*),
- śledzenie ładunków w przepływie (*cargo tracing on route*),
- bezpieczeństwo jednostek transportowych (*container/trailer security*),
- bezpieczeństwo środków transportu (*conveyance scecurity*)[14].

Organizacja, dla której bezpieczeństwo funkcjonowania stanowi jeden z priorytetów działań powinna zachęcać klientów i dostawców do podwyższania poziomu bezpieczeństwa procesów przepływu towaru i informacji oraz przedstawiać warunki współpracy w tym zakresie. Dobrą praktyką jest wymaganie od kontrahentów, aby włączali oni w realizację celów bezpieczeństwa swoje źródła zaopatrzenia. W ten sposób organizacja może oddziaływać na dalszą część łańcucha dostaw. Kluczowe znaczenie ma proces wyboru partnera gospodarczego bazujący na szczegółowych kryteriach bezpieczeństwa, w który powinna angażować się cała firma (zwłaszcza takie działy, jak import/eksport, transport, zakupy czy finanse). W sytuacji, gdy przedsiębiorstwo zmuszone jest współpra-

---

[13] B. Peleg-Gillai, G. Bhat, L. Sept, *Innovators in Supply Chain Security: Better Security Drives Business Value*, The Manufacturing Institute, Stanford University, July 2006; *The Benefits of a Secure Supply Chain*, Industry Week/IW, Vol. 255, No. 12, December 2006, s. 43.

[14] *Supply Chain Security Best Practices Catalog*, Customs-Trade Partnership against Terrorism (C-TPAT), U.S. Customs and Border Protection, January 2006 r.; P. Knight, *Supply Chain Security Guidelines*, IBM, September 2003; J.B. Rice, F.W. Spayd, *Investing in Supply Chain Security: Collateral Benefits*, Center for the Business of Government IBM, May 2005; *Innovators in Supply Chain Security: Better Security Drives Business Value*, The Manufacturing Institute, July 2006.

cować z dostawcą, którego wstępna ocena dała wynik nie w pełni zadowalający, wskazane jest wdrożenie dodatkowych procedur bezpieczeństwa celem zagwarantowania skutecznego nadzoru nad niepewnym kontrahentem i jego dostawami.

Dostawcy surowców, materiałów, wyrobów gotowych powinni być zobligowani do prowadzenia wewnętrznych audytów bezpieczeństwa, informowania organizacji o problemach, a także do regularnego dostarczania jej danych na temat zmian zachodzących w ich otoczeniu zewnętrznym (np. politycznym) i wewnętrznym (np. zmiany w kierownictwie, procedurach pakowania, manipulowania, składowania towaru, zmiany w kontraktach z partnerami 3PL). Od dostawców usług z pewnością wymagać należy szczegółowej oceny pracowników sezonowych, utworzenia zasad kontroli środków transportu,wdrożenia procedur numerowania/wydawania/umieszczania plomb na jednostkach transportowych oraz możliwości śledzenia ładunków w przepływie[15]. Pod nadzorem znajdować się powinni także klienci przedsiębiorstwa. Konieczne jest utworzenie baz danych odbiorców celem ich szybkiej identyfikacji. Przed rozpoczęciem realizacji zamówienia należy zweryfikować handlowe i bankowe referencje nabywcy. Wskazane jest osobiste poznanie nabywców i ocenienie stosowanych przez nich zabezpieczeń, które jeśli nie są wystarczające, mogą przesądzić o dalszej współpracy.

Ważnym elementem bezpieczeństwa w przedsiębiorstwie jest ustalenie zasad kontroli dostępu (*physical access control*) do ładunków, pomieszczeń, specjalnych stref firmy. Aspekt ten obejmuje implementację systemów kontroli wejść i wyjść pracowników oraz gości, wjazdów i wyjazdów dostaw, kontrolę czasu i częstotliwości przebywania pracowników w strefach ze szczególnie cennym towarem, a także stosowanie wykrywaczy metali (*hand hold detector*, *walk through*), np. przy wyjściach z firmy. To także ustalenie procedur awaryjnych uruchamianych w sytuacji, w której nieuprawnione osoby, środki transportu, niezidentyfikowane dostawy dostały się na teren organizacji.

Weryfikacja potencjalnych pracowników, przedstawianie zasad bezpieczeństwa (*code of conduct*) i skutków ich nieprzestrzegania osobom nowo zatrudnionym, wprowadzenie procedur dotyczących zasad kończenia pracy i zamykania firmy to działania mające na celu zapewnienie bezpieczeństwa dotyczącego personelu (*personnel security*). Wskazane jest zaimplementowanie prostych metod rozpoznawania osób przebywających na terenie firmy. Dobrą praktyką jest stosowanie bransoletek, kart identyfikacyjnych, uniformów w różnych

[15] Bezpieczeństwo jednostek transportowych (*container/trailer security*) obejmuje inspekcję, składowanie, śledzenie kontenerów i przyczep wzdłuż łańcucha dostaw. Dobrą praktyką jest stosowanie tzw. technologii Smart Box. Zapewnienie bezpieczeństwa środków transportu (*conveyance scecurity*) oznacza ochronę ładunków w przewozie. Polega na utworzeniu mechanizmów ich kontroli, sposobów alarmowania o sytuacji niebezpiecznej, zasad monitorowania czasów przepływu oraz lokalizacji ładunków przy wykorzystaniu GPS. Śledzenie ładunków w przepływie (*cargo tracing in route*) obejmuje m.in. używanie karty z kodami kreskowymi (*barcoded plastic card*). Jej regularne skanowanie w łańcuchu dostaw dostarcza firmie informację o ładunku w czasie rzeczywistym. *Supply Chain Security Best Practices Catalog…*, s. 17–27.

kolorach, co umożliwia odróżnienie pracowników od gości, a także rozpoznanie osób uprawnionych do przebywania w wydzielonych strefach firmy.

Zapewnienie organizacji ochrony fizycznej (*physical security*) wymaga wprowadzenia rozwiązań chroniących obiekt, zwłaszcza przed nieuprawnionym wejściem. Przedmiotem zainteresowania jest tu wyposażenie bram, drzwi, ogrodzeń firmy w alarmy, blokady i kamery oraz solidność materiałów, z których wykonany jest budynek. Istotną rolę odgrywa także zorganizowanie odpowiedniego oświetlenia, głównie w miejscach załadunku i rozładunku oraz wynajęcie firmy ochroniarskiej, spełniającej ściśle określone kryteria. Towar szczególnie cenny należy odpowiednio zabezpieczać, np. poprzez składowanie w metalowych klatkach. Również gospodarka odpadami powinna uwzględniać aspekt ryzyka. Dobrą praktyką jest nadzór i wywóz odpadów pod kontrolą oraz ścisłe zdefiniowanie sposobów dalszego z nimi postępowania.

Kluczowym elementem skutecznego osiągania celów bezpieczeństwa w łańcuchu dostaw jest budowanie świadomości kadry co do istoty problematyki, a także utworzenie przejrzystych zasad współpracy w relacjach dostawca–odbiorca, w tym procedur informowania o pojawiających się zagrożeniach. Pracownikom powinno zapewniać się szkolenia uwzględniające aspekty bezpieczeństwa w łańcuchu dostaw, w tym zagadnienia kradzieży, przemytu, kontroli i monitorowania dostaw, postępowania z ładunkami podejrzanymi czy raportowania sytuacji podejrzanych, np. nieznany klient zamówił dużą partię niebezpiecznych chemikaliów. Dobrą praktyką jest udostępnianie personelowi firmowych broszur z informacjami na temat bezpieczeństwa w przedsiębiorstwie, kraju i na świecie oraz umieszczanie w intranecie procedur bezpieczeństwa w kilku językach.

Inny element zapewniania bezpieczeństwa procesom przepływu dostaw i informacji stanowią tzw. zabezpieczenia proceduralne (*procedural security*) dotyczące rozpoznawania, postępowania i raportowania sytuacji zagrożenia. Obejmują zasady wysyłki dostaw oraz incydentalne zatrzymywanie, sprawdzanie (sporządzanie notatek, fotografowanie) i ewentualne usuwanie ładunków z przepływu. To niezbędne procedury bezpieczeństwa w firmie (np. rozładunku/załadunku) o charakterze prewencyjnym oraz plany awaryjne mające zastosowanie również na skalę globalnych łańcuchów dostaw. W ich zakres wchodzą procedury ochrony dokumentacji, uwzględniające system numerowania ważnych dokumentów (np. rezygnacja z numerowania dokumentów według przewidywalnej kolejności), zasady przechowywania zarchiwizowanych zapisów (np. składowanie ich w strefach *high value* magazynów), sposoby niszczenia niepotrzebnych dokumentów, zasady stosowania stempli, pieczątek, opakowań i taśm z logo firmy oraz zabezpieczania bieżących dokumentów (faktur, zamówień), np. podczas przerw w funkcjonowaniu przedsiębiorstwa.

Niezawodność procesów przepływu w łańcuchu dostaw warunkowana jest także budowaniem bezpieczeństwa informatycznego (*Information Technology security*). Stanowi ono szczególnie ważny aspekt, gdyż stosowanie technologii

informacyjnej determinuje sprawne funkcjonowanie globalnych łańcuchów dostaw. Ogromna ilość informacji przetwarzana w relacjach dostawca–odbiorca wymaga ochrony przed jej udostępnieniem, utratą lub modyfikacją. Dobrymi praktykami w tym obszarze są m.in:

- stosowanie zabezpieczeń z zakresu dostępu do komputerów, np. zmiana haseł przynajmniej raz na trzy miesiące;
- zakres udostępnianej zatrudnionemu informacji zależy od jego stanowiska pracy;
- korzystanie z wygaszaczy ekranu (*screen saver*);
- zakup urządzeń UPS (*Uninterruptible Power Supplies*);
- tworzenie kopii zapasowych danych;
- utworzenie wewnętrznego systemu do informowania się pracowników w firmie (*Virtual Private Network*), do którego dostęp zabezpieczony jest hasłem;
- przechowywanie serwerów w ognioodpornych pomieszczeniach;
- ciągłe doskonalenie systemu IT i korzystanie z fachowych usług celem regularnego identyfikowania podatności systemu i wprowadzenia dodatkowych ulepszeń[16].

Przedsiębiorstwo, w ramach *emergency preparedness/disaster recovery* powinno posiadać rozwinięty system skutecznych procedur awaryjnych. Wskazane jest utworzenie planu ciągłości dla łańcucha dostaw (*Supply Chain Continuity Plan*), na który składają się polityki oraz regularnie testowane i uaktualniane procedury bezpieczeństwa stanowiące odpowiedź, zwłaszcza na ataki terrorystyczne oraz katastrofy. Plan obejmuje współpracę z firmami z tej samej branży, partnerami gospodarczymi i władzami publicznymi w ramach identyfikowania podatności łańcucha dostaw oraz wprowadzania mechanizmów ochrony procesów przepływu dostaw i informacji w relacjach dostawca–odbiorca.

Istnieje wiele narzędzi wykorzystywanych w ramach zwiększania bezpieczeństwa w łańcuchu dostaw. Jednym z nich jest EDI (*Electronic Data Interchange*). Elektroniczna wymiana danych pozwala na zestandaryzowaną wymianę informacji, co przyspiesza procedury (np. generowanie dokumentów, kiedy dostawa została wysłana), ułatwia korzystanie z otrzymanej w relacjach dostawca–odbiorca informacji (np. podczas kontroli dostawy), obniża poziom ryzyka błędów popełnianych przez pracowników, a także zwiększa przejrzystość działań w łańcuchu dostaw. Wiele firm (np. dystrybucyjnych) decyduje się także na stosowanie technologii RFID (*Radio-Frequency IDentification*), która pozwala na otrzymywanie dokładnej informacji o czasie przyjęć i wysyłek dostaw, i w ten sposób, np. identyfikowanie opóźnień. Oznacza także sprawne i skuteczne monitorowanie ładunków w przepływie. Powszechne w użyciu są również mechanizmy lokalizowania środków transportów (*vehicle tracking system*) z wykorzystaniem GPS oraz stosowanie screeningu podejrzanych kontenerów celem sprawdzenia ich zawartości.

[16] *Supply Chain Security Best Practices Catalog…*, s. 46.

5. ZAANGAŻOWANIE PRZEDSIĘBIORSTW W BUDOWANIE BEZPIECZEŃSTWA ŁAŃCUCHA DOSTAW

Wyrazem zaangażowania organizacji w zapewnianie bezpieczeństwa procesów przepływu dostaw i informacji w relacjach dostawca–odbiorca jest dobrowolna implementacja systemu zarządzania bezpieczeństwem w łańcuchu dostaw, zgodnie z wymaganiami międzynarodowej normy ISO 28000:2007 *Specification for security management systems for the supply chain*[17], zbudowanej w myśl cyklu Plan-Do-Check-Act. Bazuje ona na procesie zarządzania ryzykiem i ma na celu utrzymanie ciągłości procesów wytwarzania i dostarczania w zmiennym otoczeniu globalnym. Dostarcza informację niezbędną do ustanowienia, wdrożenia, utrzymania i doskonalenia systemu przez każdą organizację, która chce wdrożyć system, zapewniać o zgodności z przepisami prawnymi w obszarze bezpieczeństwa oraz doskonalić swoje działania. Celem standardu jest utworzenie skutecznych mechanizmów rozpoznawania zagrożeń dla bezpieczeństwa oraz metod oceny, kontroli i ograniczania ryzyka, zwłaszcza poprzez działania prewencyjne, ale również reaktywne. Certyfikat ISO 28000 stanowi gwarancję, iż sprawy bezpieczeństwa stanowią dla przedsiębiorstwa ważny element strategii rozwoju. Tym samym zapewnia interesariuszy o wysokim poziomie bezpieczeństwa działań oraz skutecznej ochronie ładunków i informacji. Obserwuje się wzrost zainteresowania implementacją tego systemu zwłaszcza przez dostawców 3PL/4PL. Firmy te starają się kształtować zaufanie wobec oferowanych usług, szczególnie koncentrując się na demonstrowaniu spełniania międzynarodowych przepisów prawnych oraz skutecznego identyfikowania zagrożeń i analizowania ryzyka bezpośrednio związanego z procesami łańcucha dostaw zleceniodawców.

Organizacje zainteresowane są także standardami Światowej Organizacji Celnej (*World Customisation Organization* – WCO), w tym standardem WCO-SAFE (2005 r.), koncentrującym się na ochronie globalnych sieci dostaw i ułatwianiu handlu międzynarodowego[18]. Dotyczy on współpracy rządów, organów celnych i przedsiębiorstw. Międzynarodowa Organizacja Morska

[17] Norma ta została uzupełniona o ISO/PAS 20858:2004 *Ships and marine technology – maritime port facility security assessments and security plan development*; ISO/PAS 28001:2006 *Security management systems for the supply chain. Best practices for implementing supply chain security*; ISO 28003:2007 *Requirements for bodies providing audit and certification of supply chain security management systems*; ISO/PAS 28004:2006 *Security management systems for the supply chain. Guidelines for the implementation of ISO/PAS 28000.*

[18] Państwa, które nie posiadają zasobów na implementację wymagań SAFE, a chcą się im dobrowolnie podporządkować, otrzymują pomoc od krajów rozwiniętych w ramach tzw. *Columbus Programme* (2006 r.) Ma to na celu uniknięcie ryzyka wyłączenia biednych krajów z międzynarodowego handlu. *Supply Chain Security Initiatives: A Trade Facilitation Perspective*, Kommerskollegium 2008:1, National Board of Trade, 2008.

(*International Maritime Organization* – IMO) zaproponowała z kolei inny międzynarodowy standard, w formie dokumentu ISPS code[19] (*International Ship and Port Facility Code*). Obejmuje on zasady bezpieczeństwa dla dostaw i portów oraz reguluje kooperację pomiędzy rządem, administracją lokalną oraz jednostkami zaangażowanymi w wysyłkę ładunków i transport morski.

Przejawem manifestowania odpowiedzialności organizacji za bezpieczeństwo działań jest także angażowanie się jednostek w programy międzynarodowe. Po ataku na WTC (2001 r.) na świecie powstało wiele inicjatyw mających na celu zapewnienie bezpieczeństwa globalnym procesom przepływu dostaw i informacji (tab. 2).

Tabela 2

Inicjatywy bezpieczeństwa utworzone przez wybrane państwa

Region	Wybrane inicjatywy bezpieczeństwa
Ameryka Północna	USA: C-TPAT (Customs-Trade Partnership against Terrorism), CSI (Container Security Initiative), Advance Manifest Regulation (tzw. 24-hour rule), SAFE Port Act, FAST (Free and Secure Trade), ISA (Importer Self-Assessment), Secure Freight Initiative, Operation Safe Commerce-support for research, New legislation on 100 per cent scanning of containers. Kanada: PIP (Partnership in Protection), Advance Commercial Information.
AmerykaPołudniowa	BASC (Business Alliance for Secure Commerce).
Europa	CSP (The EU's Customs Security Programme), EU rules (for air freight, maritime transport and ports, land transport and rail transport of dangerous goods), Proposal to enhance supply chain security – Secure Operator, Cooperation between the USA and EU in security matters. Szwecja: Stairway and StairSec; Holandia: Quality assurance in the Netherlands.
Azja i Oceania	APEC/STAR (Asia Pacific Economic Cooperation/Secure Trade in the APEC region), UE-Chiny: Smart and Secure Trade Lane Pilot Project; Australia: Frontline, AEO (Authorized Economic Operator); Nowa Zelandia: Secure Exports Scheme; Singapur: Secure Trade Partnership; Jordania: the Golden List Program.

Źródło: opracowanie własne na podst. *Supply Chain Security Initiatives: A Trade Facilitation Perspective*, Kommerskollegium 2008:1, National Board of Trade, 2008.

[19] Dokument wydany w roku 2004 jako załącznik do konwencji SOLAS (Safety of Life at Sea Convention). W Europie obowiązkowe stosowanie niektórych elementów ISPS code przyjęto w ramach dyrektywy WE 725/2004.

Inicjatywy dotyczące bezpieczeństwa w międzynarodowych łańcuchach dostaw powstały w wielu regionach świata. Udział w nich jest dobrowolny lub obligatoryjny (regulowany przepisami prawnymi). Najbardziej znane spośród nich prywatne inicjatywy to stowarzyszenie TAPA (*Transported Asset Protection Association*), skupiające przedsiębiorców i przewoźników łańcuchów dostaw produktów *high value* oraz alians BASC (*Business Alliance for Secure Commerce*), mający na celu promowanie bezpiecznego handlu we współpracy z rządem i organizacjami międzynarodowymi. W Europie z kolei,w ramach unijnego Programu Bezpieczeństwa Celnego (*Customs Security Programme* – CSP) utworzona została, tzw. instytucja upoważnionego przedsiębiorcy (inaczej: Upoważnionego Podmiotu Gospodarczego – UPG (*Authorised Economic Operator* – AEO)[20]. O otrzymanie statusu AEO ubiegać się mogą przedsiębiorcy z siedzibą w Unii Europejskiej, zaangażowani w międzynarodowy obrót towarowy z krajami spoza UE, w tym producenci, odbiorcy instytucjonalni, przedsiębiorstwa transportowe czy agencje celne. Uzyskanie statusu AEO determinuje zwiększenie efektywności działań firmy i sprawniejszą współpracą w łańcuchu dostaw poprzez oszczędność czasu i ograniczenie biurokracji związanej z międzynarodowym handlem i transportem. Korzyści te wynikają z rzadszych kontroli ładunków i dokumentów, łatwiejszego dostępu do uproszczeń celnych, zmniejszonej liczby danych, jakie należy umieścić w deklaracjach skróconych, możliwości wcześniejszego powiadamiania firm o kontrolach ich dostaw, priorytetowego traktowania w sytuacji wytypowania przesyłki jednostki AEO do kontroli, możliwości wnioskowania przez UPG o sprawdzenie przesyłki w dowolnym miejscu[21]. Wyróżnia się trzy rodzaje statusów AEO:

1) AEOC, który oznacza łatwiejszy dostęp do uproszczeń celnych;
2) AEOS upoważniający do korzystania z ułatwień dotyczących kontroli bezpieczeństwa towaru w obrocie;
3) AEOF, który łączy ze sobą korzyści wynikające ze statusów AEOC i AEOS[22].

---

[20] Podstawa prawna: Rozporządzenie (WE) nr 648/2005 Parlamentu Europejskiego i Rady z dnia 13 kwietnia 2005 r. zmieniające rozporządzenie Rady (EWG) nr 2913/92 ustanawiające Wspólnotowy Kodeks Celny (Dz. Urz. UE L117 z 4.05.2005); Rozporządzenie Komisji (WE) nr 1875/2006 z dnia 18 grudnia 2006 r. zmieniające rozporządzenie (EWG) nr 2454/93 ustanawiające przepisy w celu wykonania Wspólnotowego Kodeksu Celnego (Dz. Urz. WE L 360 z 19.12.2006). W sytuacji wzmożonych kontroli celnych i ataków terrorystycznych, których celem są międzynarodowe łańcuchy dostaw, Wspólnota Europejska wprowadziła tzw. Poprawkę Bezpieczeństwa do Wspólnotowego Kodeksu Cywilnego.

[21] Upoważnieni przedsiębiorcy – wytyczne, Komisja Europejska, TAXUD/2006/1450, dokument z dn. 29 czerwca 2007, Bruksela.

[22] *Narzędzie szkoleniowe dla firm, dotyczące instytucji upoważnionego przedsiębiorcy AEO*. Komisja Europejska, http://ec.europa.eu/taxation_customs/common/elearning/aeo/index_en.htm#aeo_legislative_changes.

Uzyskanie statusu AEO stanowi o wiarygodności przedsiębiorstwa. Oznacza, że UPG jest wypłacalny, przestrzega wymagań standardów World Customs Organization, spełnia wymogi celne i podatkowe, a przede wszystkim skutecznie zapewnia fizyczne bezpieczeństwo personelowi, infrastrukturze technicznej, systemom informatycznym oraz towarowi w przepływie.

6. PODSUMOWANIE

Problematyka bezpieczeństwa sieci dostaw jest dziś niewątpliwie mocno aktualna. Zaangażowany jest w nią zarówno szczebel centralny, jak i jednostki gospodarcze. Na świecie prowadzonych jest wiele inicjatyw promujących zapewnianie ochrony procesom przepływu towaru i informacji. Należy zauważyć, że ich skuteczność opiera się nie tylko na implementacji procedur i zaawansowanych rozwiązań technologicznych. Warunkuje ją przede wszystkim partnerska współpraca, obejmująca ścisłą kooperację rządów oraz przedsiębiorstw i polegająca na dzieleniu się wiedzą, doświadczeniem, informacją na temat ładunków w przepływie i pojawiających się zagrożeń oraz budowaniu świadomości firmy oraz angażowaniu kontrahentów w sprawy bezpieczeństwa. Wdrażanie zasad bezpieczeństwa w łańcuchu dostaw dyktowane jest z pewnością obligatoryjnością przepisów prawnych w tym zakresie. Podkreślić jednak należy, że przedsiębiorstwa zainteresowane są także fakultatywnym wdrażaniem najlepszych praktyk, celem demonstrowania swojej odpowiedzialności za bezpieczeństwo procesów przepływu. Taka postawa zwiększa zaufanie klientów oraz przynosi inne korzyści, m.in. w postaci redukcji kosztów ryzyka. Warto zauważyć, że w budowanie bezpieczeństwa łańcucha dostaw zaangażowany powinien być przede wszystkim lider łańcucha dostaw, szerzący kulturę zapewniania ciągłości procesów oraz dostawcy usług logistycznych (realizujący zwłaszcza procesy transportu oraz magazynowania), którzy stanowią szczególnie aktywnych uczestników sieci dostaw, w znaczącym stopniu kształtujących bezpieczeństwo procesów przepływu.

W konkluzji należy zasugerować, iż dalsze rozważania powinny iść w stronę rozpoznania najczęściej identyfikowanych przez firmy funkcjonujące w Polsce zagrożeń dla bezpieczeństwa, a także stosowanych przez jednostki gospodarcze zabezpieczeń. Jednocześnie wskazane byłoby określenie stopnia zainteresowania tych przedsiębiorstw problematyką bezpieczeństwa i rozpoznanie najbardziej istotnych dla nich obszarów bezpieczeństwa z punktu widzenia zarządzania łańcuchem dostaw, w zależności od przestrzennego zasięgu działania, wielkości firmy czy branży.

BIBLIOGRAFIA

Closs D.J, McGarrell E.F., *Enhancing Security throughout the Supply Chain*, Special Report Series, IBM Center for the Business Government, April 2004.

Closs D., Speier C., Whipple J., Voss A.M., *Framework for Protecting Your Supply Chain*, "Supply Chain Management Review", Vol. 12, No. 2, 2008.

Enterprise Risk Management Framework, COSO 2004.

Geography of Offshoring is Shifting, raport A.T. Kearney, 2009.

Innovators in Supply Chain Security: Better Security Drives Business Value, The Manufacturing Institute, July 2006.

Knight P., *Supply Chain Security Guidelines*, IBM, September 2003.

Leonard J., *How Structural Costs Imposed on U.S. Manufacturers Harm Workers and Threaten Competitiveness*, raport National Association of Manufacturers, December 2003.

Manuj I., Mentzer J.T., *Global Supply Chain Risk Management*, "Journal of Business Logistics", Vol. 29, No. 1, 2008.

Narzędzie szkoleniowe dla firm, dotyczące instytucji upoważnionego przedsiębiorcy AEO. Komisja Europejska, http://ec.europa.eu/taxation_customs/common/elearning/aeo/index_en.htm#aeo_legislative_changes.

Nowak Z., *Zarządzanie środowiskiem*, cz. 2, Wydawnictwo Politechniki Śląskiej, Gliwice 2001.

Peleg-Gillai B., Bhat G., Sept L., *Innovators in Supply Chain Security: Better Security Drives Business Value*, The Manufacturing Institute, Stanford University, July 2006.

Physical Risks to the Supply Chain, CFO Publishing Corp., February 2009.

Rice J.B., Spayd F.W., *Investing in Supply Chain Security: Collateral Benefits*, Center for the Business of Government IBM, May 2005.

Sarathy R., *Security and the Global Supply Chain*, "Transportation Journal", Vol. 45, No. 4, 2006.

Supply Chain Security Best Practices Catalog, Customs-Trade Partnership against Terrorism (C-TPAT), U.S. Customs and Border Protection, January 2006.

Supply Chain Security Initiatives: A Trade Facilitation Perspective, Kommerskollegium 2008:1, National Board of Trade, 2008.

The Benefits of a Secure Supply Chain, Industry Week/IW, Vol. 255, No. 12, December 2006.

Ustawa o działalności ubezpieczeniowej Dz. U. 2010.11.66.

William Z., Leug J.E., LeMay S.A., *Supply Chain Security: An Overview and Research Agenda*, "International Journal of Logistics Management", Vol. 19, No. 2, 2008.

www.iata.org/events/agm/2011/gallery/Pages/video-gallery.aspx?vid=7 dn. 6 czerwca 2011 r.

Zięba R., *Kategorie bezpieczeństwa w nauce o stosunkach międzynarodowych*, [w:] Bobrow D.B., Haliżak E., Zięba R. (red.), *Bezpieczeństwo narodowe i międzynarodowe u schyłku XX*, Wydawnictwo Naukowe Scholar, Warszawa 1997.

Grażyna Wieteska

SECURITY OF SUPPLY NETWORKS

(Summary)

The disturbances that we observe on the global market in recent years demonstrate the need of implementing the tools that increase the level of supply chain security. The article presents the problem of assuring the safety of the flow of goods and information in supply chain. It also points the best practices and international secure initiatives in this area starting with explaining the risk assessment issues.