Eliza Jarysz-Kamińska[1]

Systemy zarządzania bezpieczeństwem łańcucha dostaw w Polsce

Wstęp

Jakość wyrobów zapewniająca satysfakcję klienta jest wyznacznikiem długotrwałego funkcjonowania przedsiębiorstwa na rynku. Wdrażane i sprawnie funkcjonujące systemy zarządzania wpływają na możliwości doskonalenia i rozwoju procesów zachodzących w organizacjach. Jednak to globalizacja rynku, rozproszenie i rozszerzenie kanałów transportu zwróciły uwagę na konieczność identyfikacji wpływających na nie zagrożeń i ocenę ryzyka . Dlatego tak istotne w ostatnich latach staje się zarządzanie bezpieczeństwem, które to ma zapewnić bezpieczeństwo łańcucha dostaw uwzględniając wszystkie jego aspekty jak np. produkcję, przechowywanie, transport i inne.

Celem podjęcia tego rodzaju zagadnienia jest analiza dostosowania firm krajowych do wymagań rynków zagranicznych i stosowania przez nie systemów bezpieczeństwa łańcucha dostaw.

Systemy zarządzania bezpieczeństwem łańcucha dostaw

Istnieje wiele systemów zarządzania bezpieczeństwem, jednak w 2005 roku Międzynarodowa Organizacja Normalizacyjna - ISO (International Organization for Standarization) wyszła naprzeciw przedsiębiorstwom związanym z łańcuchami dostaw ustanawiając normę ISO 28000[2]. System zarządzania bezpieczeństwem łańcucha dostaw opiera się przede wszystkim na analizie czynności związanych z kontrolą łańcucha dostaw na każdym etapie procesów produkcji i dostaw. System ten może być stosowany w każdego rodzaju przedsiębiorstwie, ma zastosowanie zarówno w sektorze produkcyjnym jak i usługowym. Rekomendowany jest wszystkim przedsiębiorstwom biorącym udział w realizacji łańcucha dostaw takim jak producenci, dostawcy, przewoźnicy, spedytorzy czy agencje celne. Celem wdrożenia tego systemu jest identyfikacja i diagnoza zagrożeń, które mogą mieć negatywny wpływ na poszczególne etapy łańcucha dostaw oraz analiza i ocena ryzyka jak i wprowadzanie środków zapobiegawczych.

Norma ISO 28000:2007[1] wskazuje przedsiębiorstwu obszary najistotniejsze w procesie budowania systemu bezpieczeństwa. Dopiero rodzina norm ISO serii 28000 przedstawia wytyczne wdrożenia i rozwiązania dotyczące systemu wychodząc tym samym naprzeciw stale rozwijającym się standardom bezpieczeństwa i potrzebom w zakresie bezpieczeństwa łańcucha dostaw stale rozwijającego się handlu światowego.

Rodzina norm ISO serii 28000

Norma ISO 28000:2007 posiada liczne podobieństwa do innych systemów zarządzania jak np.: do systemu zarządzania jakością[3] ISO 9001:2000[4], zbudowana jest na bazie normy ISO 14001:2004[5] (opiera się na ocenie ryzyka i zasadzie koła Deminga PDCA w niej zastosowanych), zauważalne są w niej jednak również elementy systemu zarządzania bezpieczeństwem informacji opartego na wymaganiach normy ISO 27001:2005[6]. Innym standardem, do którego znajdujemy w niej podobieństwa, wpływającym również na poprawę poziomu bezpieczeństwa poprzez wdrażanie mechanizmów dotyczących zarządzania ciągłością działania jest norma BS 25999-2:2007. Jest ona spójna z pojęciem AEO (Authorised Economic Operator) wprowadzonym przez rozporządzenie (EU) 648/2005 Parlamentu Europejskiego i Rady z dnia 13.04.2005[7].

Norma ISO 28000:2007 wskazuje przedsiębiorstwu obszary najistotniejsze w procesie budowania systemu bezpieczeństwa. Dopiero rodzina norm ISO serii 28000 (Tabela 1.) przedstawia wytyczne wdrożenia czy rozwiązania dotyczące systemu wychodząc tym samym naprzeciw stale rozwijającym się standardom bezpieczeństwa.

---

[1] dr inż. Eliza Jarysz-Kamińska, Zachodniopomorski Uniwersytet Technologiczny w Szczecinie, Instytut Technologii Mechanicznej

[2] ISO 28000:2007 Specification for security management systems for the supply chain

[3] Zapłata S., *Zarządzanie jakością a system zarządzania bezpieczeństwem łańcucha dostaw*, „Problemy jakości:, 2008,9,26-29.

[4] PN-EN ISO 9001:2001 *System zarządzania jakością – Wymagania*, 11.09.2001, zastąpiona normą ISO 9001:2008.

[5] PN-EN ISO 14001:2005 *Systemy zarządzania środowiskowego - Wymagania i wytyczne stosowania*, 15.03.2005.

[6] ISO/IEC 27001:2005 *Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji –Wymagania*, 14.10.2005.

[7] Official Journal of the European Union L 117/13, 4.5.2005, Strasburg.

Tabela 1. Rodzina norm ISO serii 28000

Lp.	Oznaczenie normy	Tytuł normy	Zakres normy
1	ISO/PAS 28000:2005, ISO 28000:2007	Specification for security management systems for the supply chain System Zarządzania Bezpieczeństwem Łańcucha Dostaw- wymagania	Obejmuje ona między innymi analizę ryzyka w zakresie bezpieczeństwa łańcucha dostaw, opracowanie programów bezpieczeństwa i systemowe podejście do zarządzania dostawami, co ma na celu podwyższanie poziomu bezpieczeństwa organizacji.
2	ISO/PAS 28001: 2006	Security management systems for the supply chain. Best practices for implementing supply chain security, assessments and plans. Requirements and guidance. Systemy Zarządzania Bezpieczeństwem Łańcucha Dostaw- najlepsze praktyki realizacji zabezpieczania łańcucha dostaw, jego oceny i planowania. Wymagania i wytyczne	Określa wymagania i zapewnia doradztwo dla organizacji w zakresie: opracowanie i wdrożenie procesów uwzględniających bezpieczeństwo łańcucha dostaw; ustalania i udokumentowania minimalnego poziomu bezpieczeństwa w łańcuchu dostaw lub segmentu łańcucha dostaw; wspiera AEO w ustalaniu kryteriów i zgodności krajowych programów bezpieczeństwa łańcucha dostaw. Zawiera: aneks A – Bezpieczeństwo w Łańcuchu Dostaw, aneks B – Metodologia identyfikacji i analizy ryzyk (8 kroków),
3	ISO/PAS 28002:2010, ISO 28002:2011	Security management systems for the supply chain - Development of resilience in the supply chain - Requirements with guidance for use. Systemu Zarządzania Bezpieczeństwem Łańcucha Dostaw- Rozwój odporności w łańcuchu dostaw – Wymagania i wytyczne stosowania	Określa wymagania dla systemu zarządzania odpornością w celu umożliwienia organizacji rozwoju, realizacji polityki, celów i programów z uwzględnieniem regulacji prawnych i innych wymagań do których organizacja się zobowiązała, zawiera informacje na temat ryzyk, niebezpieczeństw i zagrożeń wpływających na organizację, jej udziałowców czy łańcuch dostaw oraz ochrony majątku i procesów.
	ISO/PAS 28003: 2006, ISO 28003:2007	Security management systems for the supply chain - Requirements for bodies providing audit and certification of supply chain security management systems Wymagania do auditowania i certyfikacji Systemu Zarządzania Bezpieczeństwem Łańcucha Dostaw,	Określa zasady i wymagania w stosunku do jednostek prowadzących audity i certyfikację systemów zarządzania bezpieczeństwem łańcucha dostaw, zapewniające kompetentność i niezależność tych jednostek. Określa minimalne wymagania wobec jednostki certyfikującej i związanych z nią auditorów, podkreślając potrzebę zachowania poufności podczas kontroli i certyfikacji w firmie klienta.
5	ISO/PAS 28004:2006, ISO 28004:2007	Security management systems for the supply chain - Guidelines for the implementation of ISO 28000. Wytyczne do wdrożenia Systemu Zarządzania Bezpieczeństwem Łańcucha Dostaw.	Zawiera ogólne rady pomagające wdrożyć system ISO 28000, określa zasady systemu, opisuje typowe dane wejściowe i wyjściowe dla każdego z wymagań systemu.

Źródło: Opracowanie własna na podstawie informacji International Organization for Standardization, www.iso.org

Poza wymienionymi normami do rodziny norm odnoszących się do bezpieczeństwa łańcuchów dostaw należy zaliczyć[8]:

- ISO 20858:2007 Ships and marine technology - Maritime port facility security assessments and security plan development, wydana 17.03.2011,
- ISO 28005, Ships and marine technology – Computer applications - Electronic port clearance (EPC); jest to norma w trakcie opracowywania, podzielono ją na dwie części:
  - ISO 28005-1: Security management systems for the supply chain - Electronic port clearance (EPC) - Part 1: Message structures, publikacja planowana jest na 2014 rok,
  - ISO 28005-2:2011 Security management systems for the supply chain - Electronic port clearance (EPC) - Part 2: Core data elements, wydaną 25.02.2011,
- W opracowaniu jest również norma ISO 28006 Security management of RO-RO passenger ferries – best practices for application of security measures[9].

[8] www.iso.org.
Urbaniak M., *Zarządzanie jakością, środowiskiem oraz bezpieczeństwem w praktyce gospodarczej*, Centrum Doradztwa i Informacji Diffin Sp. z o.o., 2007, Warszawa.

[9] Wheatley Ken, *Organization for international standardization technical committee tc8,* Ships and Marine Technology, October 2009, Newsletter Issue No.23.

Wymagania i wskazówki zawarte w normie ISO 28001:2007

Norma ISO 28001:2007 wymaga stosowania praktyk w zakresie bezpieczeństwa, które zostaną ustanowione i wdrożone w celu zmniejszenia zagrożenia dla międzynarodowego łańcucha dostaw.

Spośród wymagań zawartych w normie możemy wyróżnić: „Organizacja powinna[10]…:

- dokonywać okresowo oceny bezpieczeństwa i jej wyniki dokumentować i przechowywać,
- ustanowić, wdrożyć i utrzymywać procedury dotyczące identyfikacji istniejących środków zaradczych w celu zmniejszenia zagrożeń (scenariusze). Dla każdego scenariusza zagrożeń, organizacja dokonuje oceny istniejących środków zaradczych i określa prawdopodobieństwa i istotne konsekwencje,
- udokumentować informacje obejmujące: wszystkie scenariusze zagrożenia bezpieczeństwa, metody wykorzystywane w ocenie tych zagrożeń, wszystkie środki zaradcze określone i priorytetowe,
- opracowywać i utrzymywać plany bezpieczeństwa dla wszystkich elementów łańcucha dostaw,
- ustanowić system zarządzania dla umożliwienia realizacji specyficznych procesów bezpieczeństwa łańcucha dostaw,
- opracować i utrzymywać procedury dotyczące monitorowania i oceny skuteczności systemu zarządzania oraz przeprowadzać jego audity w zaplanowanych odstępach czasu w celu zapewnienia, że został on prawidłowo wdrożony i utrzymywany,
- przeprowadzić przegląd planu bezpieczeństwa po wystąpieniu incydentu odnoszącego się do którejkolwiek części międzynarodowego łańcucha dostaw. Przegląd ten ma ustalić przyczyny zdarzenia i działania naprawcze oraz określić skuteczność środków i procedur,
- wdrożyć system zarządzania bezpieczeństwem informacji.

Wśród wytycznych zawartych w normie ISO 28001:2007 jest opracowanie planu bezpieczeństwa. Plan ten powinien obejmować między innymi[11]:

- opis łańcucha dostaw,
- wykaz obowiązków związanych z bezpieczeństwem dla wszystkich pracowników ochrony,
- struktury zarządzania bezpieczeństwem,
- opis umiejętności i wiedzę personelu odpowiedzialnego za ochronę, wykaz programów szkolenia z zakresu bezpieczeństwa,
- opis procesu kwalifikacji gwarantującego, że personel posiada niezbędne umiejętności i wiedzę do wykonywania zadań,
- wykaz alarmów próbnych, ćwiczeń dla pracowników organizacji, które można wykorzystać do spełnienia tych wymogów.

Norma ISO 28001:2007 określa również proces postępowania w ramach oceny ryzyka i rozwoju, który powinien przebiegać według następującej kolejności działań:

- określenie zakresu działalności,
- identyfikacja stosowanych form kontroli bezpieczeństwa,
- określenie scenariuszy zagrożeń bezpieczeństwa,
- określenie konsekwencji, jeśli scenariusz został zakończony,
- określenie jakie jest prawdopodobieństwo takiej sytuacji biorąc pod uwagę aktualny stan bezpieczeństwa,
- określeniu czy zastosowano wystarczające środki bezpieczeństwa,
- ewentualne wdrożenie dodatkowych środków bezpieczeństwa.

Aneks B normy ISO 28001:2007 omawia osiem kroków identyfikacji i analizy ryzyka:

1) Krok pierwszy - rozpatrzenie scenariuszy zagrożeń bezpieczeństwa (np. przejęcie kontroli nad aktywami w łańcuchu dostaw, przemyt, manipulacja, nieautoryzowane użycie).
   W ramach oceny należy wziąć pod uwagę kontrolę dostępu, środki transportu, formę transportu, formy obsługi, pracowników, komunikację wewnętrzną i zewnętrzną, firmy współpracujące, instrukcje zapobiegania wadom przesyłek, informacje zewnętrzne.
2) Krok drugi - klasyfikacja konsekwencji; ocena skutków powinna uwzględniać potencjalne straty w ludziach i straty ekonomiczne.
3) Krok trzeci - klasyfikacja prawdopodobieństwa wystąpienia incydentów związanych z bezpieczeństwem.
4) Krok czwarty - punktacja incydentu bezpieczeństwa.
5) Krok piąty - analiza środków zaradczych.
6) Krok szósty - wdrażanie środków zaradczych.

[10] ISO 28001:2007 *Security management systems for the supply chain. Best practices for implementing supply chain security, assessments and plans. Requirements and guidance,* International Organization for Standarization, 2007.

[11] ISO 28001:2007 *Security management systems for the supply chain. Best practices for implementing supply chain security, assessments and plans. Requirements and guidance,* International Organization for Standarization, 2007.

7) Krok siódmy - ocena środków zaradczych.
8) Krok ósmy - powtórzenie procesu.

Przegląd istniejących w organizacji środków bezpieczeństwa

Norma ISO 28001:2007 zawiera listę pytań na jakie musi odpowiedzieć sobie przedsiębiorstwo przy wprowadzaniu narzędzi oceny bezpieczeństwa w łańcuchu dostaw. Stanowią one podstawę przeglądu stosowanych w przedsiębiorstwie środków bezpieczeństwa. Analiza stanu faktycznego wspiera decyzje organizacji przy ocenie bezpieczeństwa łańcucha poprzez wskazanie, które elementy są wdrożone, stosowane bądź częściowo spełnione. W przypadku przedstawionych pytań dotyczących organizacji współpracujących należy określić czy spełniają wymagania niniejszej normy lub normy ISO/PAS 20858, czy posiadają międzynarodowe certyfikaty, świadectwa, zezwolenia bądź czy są wyznaczone jako AEO zgodnie z wymaganiami krajowej agencji celnej w zakresie bezpieczeństwa łańcucha dostaw.

Lista pytań została podzielona na 7 grup czynników[12]:

1) Zarządzanie bezpieczeństwa łańcucha dostaw

- Czy organizacja posiada system zarządzania, który odnosi się do łańcucha dostaw?
- Czy organizacja wyznaczyła osoby odpowiedzialne za bezpieczeństwo łańcucha dostaw?

2) Plan zabezpieczeń

- Czy organizacja posiada aktualny plan zabezpieczeń?
- Czy plan zabezpieczeń stosowany w organizacji spełnia oczekiwania partnerów biznesowych?
- Czy organizacja posiada systemy zarządzania kryzysowego, zarządzania ciągłością działania i plan budowania bezpieczeństwa?

3) Aktywa bezpieczeństwa (majątek własny zabezpieczeń)

- Czy organizacja posiada środki:
  - fizycznego zabezpieczenia budynków,
  - służące do monitorowania i kontrolowania na zewnętrz i wewnątrz terenu firmy,
  - kontroli dostępu, które zakazują nieautoryzowanego dostępu do urządzeń, środków transportu, doków załadunkowych oraz na tereny cargo, odpowiednio zastosowane środki kontroli nad identyfikacją osób (pracownik, gość, dostawca, itp.) i dostępu do innych urządzeń?
- Czy wprowadzono zabezpieczenia, które znacznie zwiększają ochrony aktywów? Na przykład, wykrywania włamań, lub nagrania kamer obejmujących obszary ważne dla funkcjonowania łańcucha, czy nagrania te przechowywane są przez dostatecznie długi okres czasu.
- Czy istnieją protokoły ze spotkań między pracownikami ochrony oraz organów zewnętrznych potwierdzające formy egzekwowania prawa w przypadku naruszenia bezpieczeństwa?
- Czy istnieją procedury w celu ograniczenia, wykrywania i zgłaszania nieuprawnionego dostępu do wszystkich towarów i magazynów?
- Czy osoby odpowiedzialne za dostarczanie i odbieranie ładunków identyfikują go w trakcie otrzymania lub wydawania?

4) Pracownicy ochrony

- Czy organizacja posiada procedury oceny rzetelności pracowników przed zatrudnieniem i okresowo w stosunku do ich zakresu zadań?
- Czy organizacja przeprowadza odpowiednie szkolenia, aby pomóc pracownikom przy wykonywaniu obowiązków związanych z bezpieczeństwem np.: utrzymanie niepodzielności ładunku, rozpoznanie wewnętrznych zagrożeń dla bezpieczeństwa i kontroli dostępu?
- Czy organizacja zapoznaje pracowników z istniejącymi w firmie procedurami w celu zgłaszania podejrzanych przypadków?
- Czy system kontroli dostępu identyfikuje wszystkich pracowników firmy poprzez dowód tożsamości i umożliwia natychmiastowe ograniczenie dostępu do obszarów wrażliwych i systemów informatycznych?

5) Bezpieczeństwo informacji

- Czy procedury stosowane w celu zapewnienia, że wszystkie informacje wykorzystane w trakcie obsługi ładunku, zarówno elektroniczne i w formie papierowej, są czytelne, aktualne, dokładne i chronione przed zmianami, utratą lub wprowadzeniem błędnych danych?
- Czy organizacja wysyłki lub odbioru ładunku jest zgodna z odpowiednią dokumentacją wysyłki ładunku?
- Czy organizacja zapewnia, że informacje dotyczące ładunku otrzymane od partnerów handlowych są dokładne i podawane we właściwym czasie?
- Czy w trakcie wykorzystywania danych są one chronione w wykorzystywanych systemach przechowywania (czy dane wracają z powrotem w miejsce procesu)?
- Czy wszyscy użytkownicy mają unikatowy identyfikator (ID użytkownika) do ich wyłącznego

[12] ISO 28001:2007 *Security management systems for the supply chain. Best practices for implementing supply chain security, assessments and plans. Requirements and guidance.*

wykorzystania, w celu zapewnienia, że ich działania można przypisać do nich?
- Czy stosowany jest skuteczny system zarządzania hasłami pracowników i czy to użytkownicy muszą zmienić hasła uwierzytelniania, co najmniej raz rocznie?
- Czy istnieją zabezpieczenia przed niepowołanym dostępem do nadużycia informacji?

6) Towary i bezpieczeństwo przewozu
- Czy istnieją procedury w celu ograniczenia, wykrywania i zgłaszania nieuprawnionego dostępu do wszystkich wysyłek, załadunku w portach i zamkniętych przewozów towarowych?
- Czy do nadzorowania przewozów towarowych wyznaczony został odpowiednio wykwalifikowany personel?
- Czy istnieją procedury dotyczące zawiadamiania właściwych organów ścigania w przypadkach nieprawidłowości lub nielegalnych działań wykrytych lub podejrzewanych przez organizację?
- Czy istnieją procedury w celu zapewnienia prawidłowego stanu towarów/ ładunku, gdy są one dostarczane do innej organizacji (transport dostawcy, centrum konsolidacji, obiektu intermodalnego, itp.) w zakresie łańcucha dostaw?
- Czy zidentyfikowano procesy śledzące zagrożenia zmiany zachodzące w trakcie transportu?
- Czy istnieją reguły bezpieczeństwa, procedury lub wytyczne przewidziane do transportu operatorów (np. w celu uniknięcia niebezpiecznych tras)?

7) CTU - szczelnie zamknięta jednostka transportu towarowego
- Jeśli wykorzystywana jest całkowicie zamknięta forma transportu to, czy istnieją udokumentowane procedury umieszczania i opisania zabezpieczeń uszczelnienia mechanicznego zgodnego z ISO / PAS 17712 i / lub innych form wykrywanie sabotażu przez personel?
- Jeśli wykorzystywana jest całkowicie zamknięta forma transportu, czy są udokumentowane procedury w celu sprawdzenia uszczelnień i zmian powstałych w trakcie przesyłki oraz gdzie odnotowywane są wykryte rozbieżności?
- Jeśli wykorzystywana jest całkowicie zamknięta forma transportu, to czy jest spoiwo sprawdzane pod kątem zanieczyszczenia tuż przed uszczelnieniem?
- Jeśli wykorzystywana jest całkowicie zamknięta forma transportu to, czy istnieją udokumentowane procedury przeprowadzania kontroli wykonawcy bezpośrednio przed uszczelnieniem w celu sprawdzenia jego rzetelności, aby móc określić niezawodność mechanizmów blokowania? Zaleca się przeprowadzenie procesu kontroli w siedmiu punktach: ściana przednia, lewa strona, prawa strona, podłoga, sufit / dach, wewnątrz / na zewnątrz zamknięcia, zewnętrzna strona/ podwozie.

Korzyści z wdrożenia systemu zarządzania bezpieczeństwem łańcucha dostaw

Wiarygodność przedsiębiorstw funkcjonujących w łańcuchach dostaw jest podstawą podjęcia współpracy w każdego rodzaju sektorze czy to transportu, spedycji czy logistyki. Wdrożenie systemu zarządzania bezpieczeństwem łańcucha dostaw jak i certyfikacja takiego systemu potwierdzają zdolność posiadającej go organizacji do zapewnienia odpowiedniego poziomu bezpieczeństwa łańcucha dostaw, eliminując możliwości jego przerwania.

Wdrożenie normy ISO 28000:2007 wpływa nie tylko na pozytywny wizerunek przedsiębiorstwa ale zapewnia satysfakcję klientów, ponadto pozwala na:
- połączenie istniejących standardów bezpieczeństwa w jeden zintegrowany system, zintegrowanie z funkcjonującymi w firmie systemami zarządzania (np. zarządzania jakością),
- ocenę ryzyka - zidentyfikowania ryzyka i punktów krytycznych zagrożeń oraz wprowadzenie ich mierników, ochrony aktywów,
- optymalizację procesów w celu zapewniania niezawodności łańcucha dostaw poprzez zapewnienie ciągłości dostaw czy skrócenie czasu dostawy,
- okazanie klientom, że przedsiębiorstwo jest zaangażowanym, świadomym i profesjonalnym partnerem,
- zwiększenie satysfakcji klientów i współpracy gospodarczej w ramach łańcucha dostaw, zwalczanie kradzieży, przemytu czy ataków terrorystycznych ,
- przygotowanie przedsiębiorstwa do uzyskania statusu AEO „Authorised Economic Partner" skutkującego w odniesieniu do kontroli celnych : zmniejszeniem liczby kontroli fizycznych i kontroli dokumentów, uprawnieniem do wcześniejszego powiadomienia o kontroli, składaniem skróconej deklaracji z ograniczonym zakresem danych bezpieczeństwa czy możliwością wnioskowania o przeprowadzenie kontroli w innym miejscu niż urząd celny[13],

[13] www.service.dekra.de.

- spójność ze standardami zabezpieczeń jak AEO i C-TPAT (The Customs-Trade Partnership Against Terrorism)[14].

Badania przeprowadzone przez Massachusetts Institute of Technology w czerwcu 2006 roku potwierdziły, że stosowanie przez firmy systemu zarządzania bezpieczeństwem łańcucha dostaw osiągnęły następujące zyski[15]:
- o 48% zmniejszono inspekcję (szybka ścieżka odpraw GREEN LANE),
- o 50% poprawiono identyfikowalność zasobów,
- o 31% skrócono czas rozwiązywania problemów,
- o 38% zredukowano straty z tytułu kradzieży.

Systemy zarządzania bezpieczeństwem łańcucha dostaw w Polsce

System zarządzania bezpieczeństwem łańcucha dostaw w Polsce nie jest powszechnie stosowany. Od początku wprowadzenia tego standardu przez ISO certyfikat poświadczający wprowadzenie i stosowanie tego systemu uzyskały cztery organizacje w kraju. Wykaz przedsiębiorstw funkcjonujących w Polsce oraz zakres stosowanych w nich systemów zarządzania bezpieczeństwem łańcucha dostaw przedstawia (Tabela 2.)

Świadczeniem usług certyfikacji ISO 28000 zajmują się w Polsce takie przedsiębiorstwa jak:
- DEKRA Certification Sp.z o.o.,
- Bureau Veritas Certification Polska,
- ISOQAR CEE Sp. z o.o.,
- Germanischer Lloyd Industrial Services Polska Sp.z o.o,
- Lloyd's Register (Polska) Sp. z o.o..

Przedsiębiorstwa te oferują wsparcie w ramach procesu wdrażania systemu zarządzania bezpieczeństwem łańcucha dostaw. Na rynku szkoleń w zakresie auditora systemu zarządzania bezpieczeństwem łańcucha dostaw bądź pełnomocnika ISO 28001 czy procesu wdrażania systemu możemy korzystać również z usług następujących firm:
- Centrum Doskonalenia Zarządzania MERITUM Sp. z o.o.,
- Qualita Perfecta,
- PBSG Sp. z o.o.,
- LRQA Polska Business Assurance.

Koszty szkoleń wahają się w granicach 1300-1800 zł za kurs dwudniowy. Koszty doradztwa w ramach oceny systemu zarządzania, szkolenia personelu, tworzenia dokumentacji wdrażania działań, analizy i oceny ryzyka zależne są od wielkości organizacji.

Tabela 2. Wykaz firm posiadających certyfikat ISO 28000 w Polsce

Nazwa certyfikowanej organizacji	Data wydania certyfikatu	Zakres systemu	Organizacja certyfikująca
Security Plus Sp. z o.o. ul. Arkuszowa 39, 01-934 Warszawa	6 stycznia 2009	Świadczenie usług zapewnienia bezpieczeństwa, włączając ocenę doradztwo i ochronę.	Lloyd's Register (Polska) Sp. z o.o. w imieniu Lloyd's Register Quality Assurance Limited
Action S .A. Jana Kazimierza 46/54, 01–248 Warszawa	4 października 2010	Handel i dystrybucja towarów branży teleinformatycznej, AGD, RTV i materiałów eksploatacyjnych. Produkcja (w zakresie projektowania konfiguracji, montażu, testowania i serwisu) zestawów komputerowych.	Germanischer Lloyd Industrial Services Polska Sp. z o.o 00-876 Warszawa
Solid Logistics Sp. z o.o., z siedzibą w Warszawie, ul. Smoleńskiego 4/18, 01-698 Warszawa	1 maja 2009	Spedycja morska, spedycja drogowa, spedycja lotnicza, logistyka magazynowa i usługi celne.	Germanischer Lloyd Industrial Services Polska Sp.z o.o 00-876 Warszawa
Flextronics Logistics Poland Sp. z o.o. Ofiar Terroryzmu 11 Września 17, 92-410 Łódź	2 października 2008	Magazynowanie, ewidencja, zwiększanie wartości i prowadzenie działalności centrum logistyki odwrotnej w Łodzi, w tym transfer zasobów materialnych do innych oddziałów Flextronics i	Lloyd's Register (Polska) Sp. z o.o. w imieniu Lloyd's Register Quality Assurance Limited

Wnioski

[14] http://www.bureauveritas.pl.
[15] Sitkowski L., *Zarządzanie bezpieczeństwem dla łańcucha dostaw-ISO28000*, Przemysł i Środowisko. Jakość - Zarządzanie, 4(13)2009.

Rozwój przedsiębiorstw, zwiększanie zasięgu działalności, liczby odbiorców czy dróg dystrybucji towarów zwiększa możliwość występowania czynników niebezpiecznych w łańcuchu dostaw. Konieczność zapewnienia odpowiedniej jakości produktu, stabilności zawartych umów oraz dostaw, bezpieczeństwa
i terminowości transportu powoduje, że łańcuchy dostaw są coraz bardziej narażone na niebezpieczeństwo ich przerwania. Wzrasta możliwość wystąpienia zagrożeń takich jak: zakłócenia i opóźnienia w dostawie, możliwość ataku terrorystycznego, przemytu, uszkodzenie towaru, rosnące koszty obsługi, brak bezpieczeństwa personelu, błędny przepływ danych, nieadekwatne moce produkcyjne, utrata własności intelektualnej i awarie systemów informatycznych. Jednak próba wyeliminowania tych zagrożeń poprzez wdrożenie systemu zarządzania bezpieczeństwem łańcucha dostaw według wymagań normy ISO 28000:2007, którego celem jest zapewnienie odpowiedniego poziomu bezpieczeństwa, poprzez wdrożenie i utrzymanie zabezpieczeń przez każdego uczestnika łańcucha nie jest szeroko rozpowszechnione w naszym kraju. System ten mimo że ukierunkowany jest na bezpieczeństwo zasobów a nie bezpośrednio na jakość jest odpowiedzią na problem analizy i oceny zagrożeń firm działających w branży transportowej, spedycji czy logistyki. Duża ilość zagrożeń wpływających na łańcuch dostaw przyczyni się do tego, że system zarządzania bezpieczeństwem łańcucha dostaw stanie się równie popularny jak system zarządzania jakości w dążeniu do samodoskonalenia organizacji i satysfakcji klienta.

Streszczenie

Artykuł zawiera prezentację rodziny norm ISO serii 28000 dotyczących systemu zarządzania bezpieczeństwem łańcucha dostaw. Omówione zostaną wymagania i wskazówki zawarte w normie ISO 28001:2007 System zarządzania bezpieczeństwem łańcucha dostaw – najlepsza praktyka wdrażania oraz lista pytań na jakie musi odpowiedzieć sobie przedsiębiorstwo przy wprowadzaniu w organizacji narzędzi oceny bezpieczeństwa w łańcuchu dostaw. Ponadto przedstawione zostaną korzyści z certyfikacji omawianego systemu oraz zakres tego rodzaju praktyk w Polsce.

Abstract

The paper presents series of standards ISO 28000 - Security management systems for the supply chain. The requirements and guidance contained in standard ISO 28001:2007 "Security management systems for the supply chain – Best practices for implementing supply chain security" will be discussed and also performance review list which the organization must answer in the implementation of security assessment for the supply chain. Furthermore, the paper will present the benefits of the system certification and the range of such practices in Poland.

Literatura

1. *Certyfikacja ISO 28000*, http://www.bureauveritas.pl/wps/wcm/connect/bv_pl/Local/Home/bv_com_serviceSheetDetails?serviceSheetId=14421&serviceSheetName=Certyfikacja+ISO+28000+%2528wersja+angielska%2529, dostęp 20.06.2011.
2. *ISO 28000 Zarządzanie bezpieczeństwem łańcucha dostaw,* http://www.service.dekra.de/intertek/show.php3?id=1840&nodeid=1840&p=0&_language=pl, dostęp 20.06.2011.
3. ISO 28000:2007 *Specification for security management systems for the supply chain,* International Organization for Standardization, 2007.
4. ISO 28001:2007 *Security management systems for the supply chain. Best practices for implementing supply chain security, assessments and plans. Requirements and guidance,* International Organization for Standarization, 2007.
5. Official Journal of the European Union, *L 117/13*, 4.5.2005, Strasburg.
6. Sitkowski L., *Zarządzanie bezpieczeństwem dla łańcucha dostaw- ISO 28000*, „Przemysł i Środowisko. Jakość – Zarządzanie", 2009, 4(13), 28-29.
7. Urbaniak M., *Zarządzanie jakością, środowiskiem oraz bezpieczeństwem w praktyce gospodarczej*, Centrum Doradztwa i Informacji Diffin Sp. z o.o., 2007, Warszawa.
8. Wheatley Ken, *Organization for international standardization technical committee tc8,* "Ships and Marine Technology", October 2009, Newsletter Issue No.23.
9. Zapłata S., *Zarządzanie jakością a system zarządzania bezpieczeństwem łańcucha dostaw*, „Problemy jakości:, 2008,9,26-29.