Tomasz SMAL , Marian KOPCZEWSKI

INNOWACYJNOŚĆ PRZEDSIĘBIORSTW LOGISTYCZNYCH A BEZPIECZEŃSTWO INFORMACJI

Streszczenie

Celem artykułu jest przedstawienie problemów związanych z zarządzaniem informacją oraz poszukiwanie zrównoważonych relacji i właściwych proporcji pomiędzy rozwojem innowacji przedsiębiorstw logistycznych a bezpieczeństwem przetwarzanych przez nie informacji. Informacja, jako jeden z najcenniejszych zasobów przedsiębiorstwa, powinna być obiektem szczególnej troski. Dlatego też, w artykule omówiono takie kwestie związane z zarządzaniem informacją jak: rola informacji w zarządzaniu przedsiębiorstwem, a w tym składowe systemu informatycznego, normalizacja i standaryzacja analizowanych procesów, bezpieczeństwo informacji - jego składowe i organizacja oraz zarządzanie ryzykiem w systemie bezpieczeństwa informacji. Przeanalizowane zagadnienia pozwoliły wyłuszczyć najistotniejsze kwestie związane z bezpieczeństwem informacji w relacji do funkcjonowania i rozwoju przedsiębiorstw logi-stycznych.

WPROWADZENIE

Współczesne przedsiębiorstwo logistyczne funkcjonujące w konkurencyjnym środowisku powinno w sposób ciągły tworzyć (lub przejmować z otoczenia) i wdrażać różnego rodzaju innowacje zabezpieczające efektywność jego działania i rozwoju. Przedsiębiorstwa logistyczne mając do dyspozycji określony potencjał naukowy i materialny, działając pod wpływem różnych czynników i stosując dostępne innowacje, realizują postęp (społeczny, techniczny, organizacyjny, itd.), który decyduje o tempie rozwoju społeczno-gospodarczego oraz o poziomie warunków życia i pracy społeczeństwa. Postęp w zakresie innowacji jest niezbędny i nieunikniony w konkurencyjny mechanizmie rozwoju Świata. Nie możemy jednak zapominać o konieczności realizowania zrównoważonego rozwoju, mającego na celu uchronić świat przed nieprzemyślanymi i zbyt szybkimi wdrożeniami innowacji, które mogą przynieść tragiczne skutki dla ekologii i życia społecznego.

Współczesne przedsiębiorstwa, aby w przyszłości skutecznie konkurować na rynku, powinny systematycznie śledzić i analizować trendy rozwoju techniki, organizacji, zarządzania (gdzie podstawą jest informacja) oraz odpowiadać na imperatyw innowacji, a także reagować na zmiany w zakresie realizowania procesów logistycznych. Chodzi też o to, aby przedsiębiorstwa miały możliwość tworzenia innowacji zgodnie z potrzebami społecznymi, aby zaistniały warunki do szybkiej dyfuzji innowacji w skali przedsiębiorstwa. Wprowadzenie innowacji powinno być również jednym z celów strategicznych przedsiębiorstwa. P.F. Drucker pisze, że przedsiębiorstwo nie wprowadzające innowacji nieuchronnie starzeje się i podupada. W okresie gwałtownych zmian w zakresie funkcjonowania przedsiębiorstw, takim jak obecnie, ewentualny upadek spowodowany brakiem innowacyjności, będzie jeszcze szybszy. Można zatem stwierdzić, że procesy innowacyjne w odpowiednio dobranej strategii przedsiębiorstwa są podstawowym czynnikiem jego rozwoju. Mówiąc o roli innowacji w rozwoju przedsiębiorstwa należy mieć na myśli nie tylko jego technologiczno - informacyjny aspekt, ale również rozwój organizacyjny, ekologiczny, ekonomiczny, społeczny itd., czyli ogólnie mówiąc zrównoważony.

W warunkach gospodarki rynkowej pojawiają się sprzyjające przesłanki do wzrostu innowacyjności przedsiębiorstw logistycznych. Istnieją realne możliwości dla formowania nowego typu rozwoju. Pod pojęciem innowacyjnego typu rozwoju rozumiemy proces przejścia jednostek w całości w nowy jakościowo stan w oparciu o innowacje technologiczne, ekologiczne, organizacyjne i inne, zabezpieczające bardziej efektywny i dynamiczny rozwój. Osobliwością innowacyjnego typu rozwoju przedsiębiorstw logistycznych jest to, że działa w nim kompleksowo duża grupa różnorodnych czynników dających synergiczny efekt. Nie przeciwstawia się jednego typu rozwoju innemu. Intensywny typ rozwoju przy określonych warunkach przechodzi w innowacyjny.

Jedną z największych wartości jakie obecnie posiadają przedsiębiorstwa, w tym te oferujące usługi logistyczne, jest informacja. Dzięki informacji, firmy mogą przewidywać zachowania rynku, realizować usługi czy też planować i kreować ruchy gospodarcze w przyszłości. Niemal z dnia na dzień informacja stała się bardzo cennym narzędziem gospodarczym. Wraz ze wzrostem jej wartości pojawiły się problemy dotyczące jej ochrony oraz zabezpieczenia przed nieuprawnionym do niej dostępem osób nieupoważnionych.

Głównym celem artykułu jest ukazanie znaczenia bezpieczeństwa informacji w funkcjonowaniu przedsiębiorstwa logistycznego, a szczególnie jej wpływu na jego innowacyjność.

1. BEZPIECZEŃSTWO INFORMACJI JAKO ZNACZĄCY ELEMENT STRATEGII BEZPIECZEŃSTWA PRZEDSIĘBIORSTWA

W tak szybko zmieniającym się świecie i eksplozji rozwoju technologii, ochrona informacji stała się nie tylko coraz większym wyzwaniem ale i koniecznością. Dla wielu przedsiębiorstw zapewnienie bezpieczeństwa posiadanych danych stało się kluczowym zagadnieniem biznesowym. Starania mające na celu zagwarantowanie bezpieczeństwa informacji przypominają dziś wyścig z czasem, ponieważ tak szybki rozwój technologiczny w zakresie przepływu danych jest praktycznie nie do opanowania. Ponadto, technologie informatyczne są stosowane w coraz bardziej newralgicznych przypadkach, a co za tym idzie ich znaczenie również dla bezpieczeństwa staje się bardziej istotne. Istotą zabezpieczenia teleinformatycznego jest zapewnienie bezwarunkowego bezpieczeństwa informacjom, które są utrzymywane, przesyłane i przetwarzane przez systemy informatyczne. Nie jest to zadanie łatwe ze względu na fakt występowania szeregu trudności i przeciwieństw.

Bezpieczeństwo informacyjne w połączeniu z bezpieczeństwem ekonomicznym staje się priorytetowym aspek-

tem w odniesieniu do bezpieczeństwa społecznego. Przemiany organizacyjne i techniczne zapoczątkowane w tamtym czasie powodują kolejne różnice między narodami i organizacjami, ale także podmiotami funkcjonującymi w globalnej gospodarce. Albowiem, w miarę upływu czasu poziom asymilacji nadciągającej rewolucji cyfrowej oraz poziom dostrzegania potrzeby przemian technologicznych stał się wyznacznikiem rozwoju w sferze ekonomicznej i gospodarczej. Rozwój technologii informacyjnej w znacznym stopniu zrewolucjonizował praktyki gospodarcze i procesy funkcjonujące w przedsiębiorstwach. Tempo przemian jest silnie uwarunkowane ekonomicznie i społecznie, a ważnymi atutami w „grze o jutro" jest aktualny potencjał gospodarczy, posiadana infrastruktura informacyjna, wielkość i dynamika rynku, innowacyjność i otwartość na zmiany. Przepływ i wymiana informacji według prognoz, staną się podstawą dla sprawnego funkcjonowania firm, administracji wszystkich szczebli oraz życia jednostek. Staną się, jak utrzymuje Alvin Toffler, „naczelnym czynnikiem wytwórczości i władzy człowieka" w społeczeństwie informacyjnym [5].

Ogólna definicja bezpieczeństwa, czyli stanu spokoju, harmonii i niezagrożonego rozwoju odnosi się zwykle do obiektu. W przypadku bezpieczeństwa informacji mamy na myśli całość systemu bezpieczeństwa informacji danej firmy czy instytucji publicznej. W skład tego zagadnienia wchodzi również całość informacji i procesów, które służą realizacji interesów firmy. Podstawowymi celami stawianymi bezpieczeństwu informacji w przedsiębiorstwie jest zapewnienie i trwanie bezpieczeństwa tego systemu w określonym czasie (Tab. 1). Bezpieczeństwo teleinformatyczne jest jednym z warunków zapewnienia bezpieczeństwa informacji, ale nie jest jedynym jego atrybutem. Rozważmy definicję bezpieczeństwa teleinformatycznego: „Bezpieczeństwo teleinformatyczne rozumiane jest jako zespół procesów zmierzających do zdefiniowania, osiągnięcia i utrzymywania założonego poziomu poufności, integralności, dostępności, rozliczalności, autentyczności i niezawodności, czyli atrybutów bezpieczeństwa w systemach teleinformatycznych" [1, s. 33].

Tab. 1. *Określenie atrybutów właściwość bezpieczeństwa na podstawie norm [8]*

Nazwa	Określenie
Poufność	Właściwość zapewniająca, że informacja nie jest udostępniona lub ujawniona nieautoryzowanym osobom, podmiotom lub procesom.
Autentyczność	Właściwość zapewniająca, że tożsamość podmiotu lub zasobu jest taka jak deklarowana; dotyczy użytkowników, procesów, systemów lub nawet instytucji; autentyczność jest związana z badaniem, czy ktoś lub coś jest tym lub czym za kogo lub za co się podaje.
Dostępność	Właściwość bycia dostępnym i możliwym do wykorzystania na żądanie w założonym czasie przez kogoś lub coś, kto lub co ma do tego prawo.
Integralność danych	Właściwość zapewniająca że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
Integralność systemu	Właściwość polegająca na tym że system realizuje swoją zamierzoną funkcję w nienaruszony sposób, wolny od nieautoryzowanej manipulacji, celowej lub przypadkowej.
Integralność	Integralność danych oraz integralność systemu.
Rozliczalność	Właściwość zapewniająca, że działania podmiotu (np. użytkownika) mogą być jednoznacznie przypisane tylko temu podmiotowi.
Niezawodność	Właściwość oznaczająca spójne, zamierzone zachowanie i skutki.

2. NORMY, STANDARDY I NARZĘDZIA WSPIERAJĄCE UTRZYMANIE I ROZWÓJ BEZPIECZEŃSTWA INFORMACJI

Wraz z rozwojem systemów teleinformatycznych dostępnych w sieci komputerowej powstała potrzeba ustandaryzowania zagadnień związanych z bezpieczeństwem tych systemów. Głównym celem standaryzacji było określenie sposobów ochrony informacji, a także oceny skuteczności działań opartych o te metody. Pierwsze przymiarki do opracowania dotyczące tej tematyki pojawiły się wraz z eksplozją technologii informacyjnych w Stanach Zjednoczonych. Pierwszym dojrzałym dokumentem była „Pomarańczowa Księga" opracowana przez Departament Obrony USA. Wraz z rozkwitem technologii rozwój standardów był rozwijany w dość żywiołowym tempie, ponadto mógł cieszyć się wsparciem zarówno społeczności międzynarodowych jak i stowarzyszeń i innych organizacji pozarządowych inspirowanych biznesem. Obecnie standardy dotyczące bezpieczeństwa informacji są stale aktualizowane, co jest wymuszone szybkim rozwojem technologicznym. W tym temacie powstaje ciągle mnóstwo opracowań wytycznych i zaleceń, które w swoich tytułach zawierają określenie „standard. W tej sytuacji jest zasadne pytanie, kiedy opracowania są standardami i czy w ich tworzeniu musza uczestniczyć oficjalne gremia normalizacyjne [1, s. 45].

Istnieje wiele standardów rozumianych jako dobre praktyki lub lokalne rekomendacje zainteresowanych środowisk branżowych lub firm audytorskich jednak najbardziej ogólny podział obejmuje standardy:

- Oficjalne – tworzone przez gremia standaryzacyjne, wśród których rozróżniamy:
  - Międzynarodowe organizacje, np. ISO (International Organization of Standardization), IEC (International Electrotechnical Commission), ITU (Telecommunication Standardisation Sector of the Internationla Telecommunications Union);
  - Regionalne organizacje, np. CEN (Commite European de Normalization), ETSI (European Telecommunications Standards Institute), NAFTA (North America Free Trade Area);
  - Krajowe organizacje ANSI (American Nations Standard Institution), SCC (Standard Council of Canada) lub PKN (Polski Komitet Normalizacyjny).
- Pozostałe – w tym wszystkie standardy obejmujące zalecenia zainteresowanych organizacji, firm i stowarzyszeń branżowych.

Praktyka pokazuje, że taki podział ma bardzo umowny charakter. Pewne rozwiązania rozwijane przez organizacje lub firmy z czasem gdy znajdują wielu zwolenników są przekazywane do organizacji normalizacyjnych w celu opracowania na ich podstawie norm oficjalnych. Tak było w przypadku sieci Ethernet lub kart elektronicznych. Z kolei można podać przykłady standardów oficjalnych, które nie przyjęły się powszechnie lub zostały wyparte przez rozwiązania firmowe [1, s. 46].

W celu zapewnienia maksymalnego bezpieczeństwa informacji, przedsiębiorstwa powinny samodzielnie poddać się kontroli i w miar w własnych możliwości starać się realizować przegląd bezpieczeń-

stwa własnych systemów i rozwiązań. Narzędziami usprawniającymi proces zautomatyzowanego przeglądu instalacji są skanery automatyczne. Skanery to rozwiązania sprzętowe i programowe które pozwalają w krótkim czasie przeprowadzić serię sprawdzeń i ataków w celu znalezienia „dziur" w oprogramowaniu lub w infrastrukturze sprzętowej. Zastosowanie tego rodzaju auto-testowania własnej infrastruktury informatycznej daje nam odpowiedź tylko cząstkową, ponieważ metoda ich działania opiera się na poszukiwaniu znanych błędów nie analizując zupełnie błędów w sposobie stosowania tego oprogramowania. Jak w wielu przypadkach tak i w sferze bezpieczeństwa informacji okazuje się że najsłabszym ogniwem jest mimo wszystko człowiek. Niemniej jednak stosowanie tego rodzaju skanerów znacznie przyspiesza proces rozpoznania i bezpieczeństwa systemu w zakresie „dziurawego" oprogramowania. Produkty te nie są trudne w użyciu i nie wymagają specjalistycznej wiedzy technicznej dzięki czemu testy tego rodzaju mogą zostać przeprowadzone nawet przez średnio wyszkolony personel techniczny. Wynikiem działania tego rodzaju skanerów są szczegółowe raporty które w dalszej części procesu weryfikacji powinny być poddane szczegółowej analizie przez odpowiednio wyszkolone osoby. Należy jednak pamiętać że mogą one wykryć jedynie znane i znajdują się w bazie zdefiniowanych błędów.

Najbardziej istotną sprawą wpływającą na jakość badania jest właśnie aktualność i kompletność bazy zdefiniowanych błędów. W trakcie stosowania automatycznych systemów wspomagających kontrolę bezpieczeństwa bardzo często firmy popełniają błędy, które w konsekwencji dają im złudne poczucie bezpieczeństwa w sytuacji kiedy stan faktyczny jest zupełnie inny. Dość popularnym błędem pojawiającym się w organizacjach jest zabezpieczenie systemów „od frontu" lecz pozostawienie otwartych „tylnych drzwi", przez które można ominąć wszystkie nawet najbardziej zaawansowane zabezpieczenia. Ważnym elementem, który należy rozważyć już na poziomie projektowania rozwiązania informatycznego jest utrzymanie optymalnego poziomu zabezpieczeń całego systemu. Nawet największe inwestycje w infrastrukturę systemów zabezpieczeń nie uchroni firmy przed niebezpieczeństwem włamania jeśli oprogramowanie działające na tych systemach będzie przestarzałe. Jak w wielu innych dziedzinach życia musimy pamiętać o tym, że system bezpieczeństwa informacji w naszej organizacji jest tak silny jak najsłabsze jego ogniwo.

Kolejnym błędem, który znacząco wpływa na obniżenie poziomu bezpieczeństwa jest brak wiedzy lub zaangażowania w dostrojeniu systemów monitorujących czy skanerów. Zainstalowanie rozwiązania „z pudełka", czyli z domyślnymi ustawieniami, nie gwarantuje nam pełnej kontroli i testów dopasowanych do naszych realiów i oczekiwań. Niestety zbyt często ufamy technologii i zapominamy o tym, że działa ona pod warunkiem spełnienia określonych założeń. Nie ma technologii uniwersalnej, która zabezpieczy wszystko. Dość często spotykamy się ze stwierdzeniem „Mam firewall, więc moja sieć jest bezpieczna". Zgadza się, że firewall zabezpieczy sieć jednak pod warunkiem, że jest on odpowiednio skonfigurowany do pracy w naszym środowisku. Innym przykładem mogą być technologie szyfrujące. Przy zastosowaniu publicznego klucza szyfrującego, np. PGP, stosuje się szyfrowanie informacji bez użycia podpisu, takie podejście nie daje nam gwarancji pochodzenia listu elektronicznego – za to odpowiada właśnie podpis. Poza tym, przy zastosowaniu technologii szyfrujących często zapominamy o zasadzie, że szyfrowana informacja jest na tyle bezpieczna na ile bezpieczne jest hasło szyfrujące. Niestety nadal częstą praktyka jest przesyłanie zaszyfrowanych informacji jako załącznik maila, w którym przesyłane jest również hasło. Tego rodzaju „zabezpieczenie" nie daje nam praktycznie żadnej gwarancji bezpieczeństwa informacji.

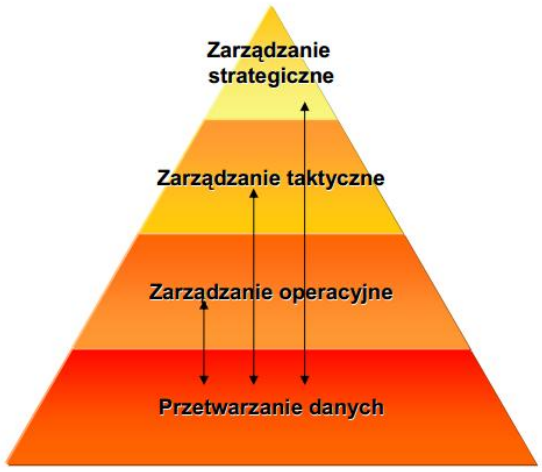
Mając na względzie wszystkie powyższe zagrożenia należy pamiętać o tym, że szkolenie pracowników, ich edukacja w zakresie zagrożeń są tym, bez czego nawet najbardziej zaawansowane systemy zabezpieczeń są bezradne.

3. INFORMACJA JAKO NAJCENNIEJSZE DOBRO W PRZEDSIĘBIORSTWIE LOGISTYCZNYM

Informacja posiada kilka różnych definicji, w zależności od dziedziny która ją opisuje skupia się ona na innych atrybutach i podkreśla różne jej znaczenie. Z punktu widzenia przedsiębiorstwa logistycznego, dla którego informacja jest lub może być znaczącym determinantem wpływającym na jego efektywność finansową, informacja powinna być: kompletna, istotna, terminowa, właściwa, wiarygodna, zrozumiała.

Powyższe przymioty są gwarantem, iż dana informacja ma dla przedsiębiorstwa znaczenie i jest dla niego istotna. W specyfice wolnorynkowej informacja ma określoną wartość w danym czasie dla danych podmiotów. Oznacza to, iż ta sama informacja w różnym czasie może mieć skrajnie różne znaczenie, w pewnych sytuacjach może przynieść firmie ogromne korzyści a w innych nie ma absolutnie znaczenia w wymiarze ekonomicznym. Z punktu widzenia podmiotu gospodarczego nastawionego na realizację celów biznesowych możemy wyróżnić cztery obszary bezpieczeństwa informacji: administracyjno-organizacyjny, formalno-prawny, techniczno-programowy, fizyczny.

Bezpieczeństwo informacji to nic innego, jak obrona informacyjna, która polega na uniemożliwieniu i utrudnieniu zdobywania danych o fizycznej naturze aktualnego i planowanego stanu rzeczy i zjawisk we własnej przestrzeni funkcjonowania oraz utrudnianiu wnoszenia entropii informacyjnej do komunikatów i destrukcji fizycznej do nośników danych. Na każdym poziomie zarządzania bezpieczeństwem informacji (Rys. 1), zasadniczym celem jest niedopuszczenie do jej ujawnienia. Należy podkreślić, że zbyt szerokie rozumienie bezpieczeństwa może utrudniać przepływ informacji w państwie, przedsiębiorstwie, itp. – informacji, które są niezbędne do ich sprawnego i skutecznego funkcjonowania [2, s. 18].



Rys. 1. *Rola informacji w zarządzaniu przedsiębiorstwem.*
Źródło: Opracowanie własne na podstawie materiałów z warsztatów „Computerword", prowadzonych przez Spółkę Ernst & Young, na temat „Rola pracownika w bezpieczeństwie informacji w firmie", Warszawa 13 stycznia 2014 r .

System monitorowania bezpieczeństwa to cały cykl działań, które tylko sprzężone w pewien określony i zaplanowany proces mają szansę zapewnić przedsiębiorstwom bezpieczeństwo informacyjne. W takim układzie cały system jest tak mocny jak najsłabsze

jego ogniwo, tym samym nie można mówić o sprawnym systemie bezpieczeństwa bez zasad, procedur czy procesów monitorowania. Proces ten dość dobrze został zobrazowany na poniższym diagramie:

Bezpieczeństwem informacyjnym jest również każde działanie, system bądź metoda, które zabezpieczają zasoby informacyjne gromadzone, przetwarzane, przekazywane oraz przechowywane w pamięci komputerów i sieciach teleinformatycznych. Dlatego też bezpieczeństwo informacyjne należy rozumieć jako wypadkową bezpieczeństwa fizycznego, prawnego, osobowo-organizacyjnego oraz teleinformatycznego organizacji gospodarczej [6, s. 80].

Na problematykę bezpieczeństwa informacji musimy patrzeć jak na proces ciągły w ramach których podmioty ekonomiczne doskonalą swoje mechanizmy obronne prowadzące do zwiększenia poczucia bezpieczeństwa. Odzwierciedlenie rozumienia i traktowania bezpieczeństwa jako kluczowego obszaru zainteresowań przedsiębiorstw znajdujemy w ich działaniach podejmowanych w obliczu zagrożenia. Działania te są zadaniami trudnymi i kosztownymi, co w wielu przypadkach niestety może stanowić przyczynę ich zaniechania.

4. ISTOTA PRZECHOWYWANIA I ZABEZPIECZANIA INFORMACJI

Zarządzanie bezpieczeństwem systemów informacyjnych ma swoje cele, których realizacja gwarantuje zwiększenie bezpieczeństwa informacyjnego przedsiębiorstwa. Cele te możemy podzielić na trzy główne obszary bezpieczeństwa:

- Wiedzieć i znać realne zagrożenia systemów informacyjnych – w tym celu należy stale identyfikować zagrożenia na jakie podatny jest system informacyjny, a także znać i ocenić ryzyka związane z bezpieczeństwem tego systemu;
- Odpowiednio zabezpieczyć system informacyjny – poprzez dobranie odpowiedniej metody zarządzania bezpieczeństwem oraz mechanizmów bezpieczeństwa, które będą adekwatne do bieżących potrzeb;
- Stale monitorować i utrzymywać przyjęty poziom bezpieczeństwa – za pomocą ciągłego monitorowania ryzyka oraz wykorzystania mechanizmów bezpieczeństwa i badania ich efektywności.

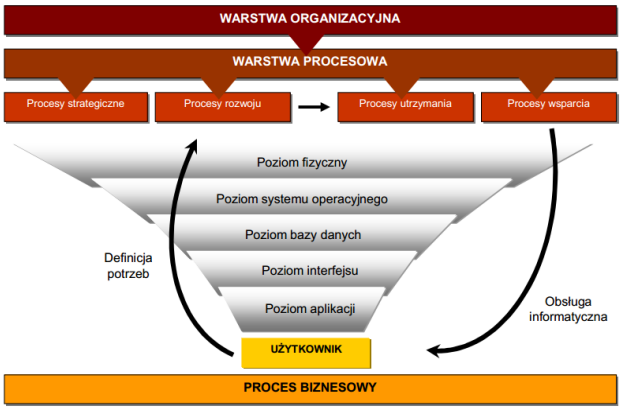
Osiągnięcie tych celów nie jest łatwą sprawą oraz nierzadko wiąże się z kosztami czy to bezpośrednio finansowymi, czy też związanymi z infrastrukturą lub koniecznością zapewnienia większych zasobów ludzkich.

Przestępstwa występujące w biznesie tworzą specyficzną grupę, ponieważ, zagrażając przedsiębiorstwom czy instytucjom, stanowią zagrożenie dla zasobów organizacji, np. dla posiadanych baz informacji, środków pieniężnych, wartości firmy, takich jak reputacja, wyrobione stosunki bądź przywileje handlowe danego przedsiębiorstwa [2, s. 268]. Pojęcie zagrożeń bezpieczeństwa informacyjnego przedsiębiorstwa można opisać przez identyfikację poniższych stref zagrożeń [4, s. 751]:

- Zagrożenia losowe – to takie gdzie dochodzi do różnego rodzaju klęsk, katastrof i wypadków które mają bezpośrednio wpływ na poziom bezpieczeństwa informacyjnego organizacji;
- Zagrożenia tradycyjne – mówimy o nich gdy mamy do czynienia z działalnością dywersyjną, sabotażem lub szpiegostwem. Celem takiego ataku jest dezinformacja lub nielegalne pozyskanie informacji;
- Zagrożenia technologiczne – to wszystkie te zagrożenia, gdzie mamy do czynienia z gromadzeniem, przechowywaniem i przetwarzaniem informacji w sieciach komputerowych. Typowym zagrożeniem tego rodzaju jest cyberterroryzm.
- Zagrożenia organizacyjne – to te wynikające z niedostatecznych rozwiązań strukturalnych, proceduralnych i organizacyjnych;

Zagrożenia bezpieczeństwa możemy podzielić również pod względem ich źródeł na:

- Zagrożenia wewnętrzne – to te, które mają miejsce wewnątrz organizacji, skutkiem których, może być utrata informacji, uszkodzenie danych, brak ciągłości biznesowej;
- Zagrożenia zewnętrzne – których źródło powstawania jest poza organizacją. W takim przypadku najczęściej mamy do czynienia z nieświadomym bądź celowym działaniem ze strony osób lub podmiotów trzecich;
- Zagrożenia fizyczne – w przypadku których dochodzi do nieoczekiwanej awarii systemu komputerowego lub sieci, co w konsekwencji nie pozwala realizować procesów biznesowych opartych o systemy informatyczne.
-



Rys. 2. *Składowe systemu informatycznego i ich znaczenie dla procesu biznesowego przedsiębiorstwa logistycznego*
Źródło: Opracowanie własne na podstawie materiałów z warsztatów „Computerword", prowadzonych przez Spółkę Ernst & Young, na temat „Rola pracownika w bezpieczeństwie informacji w firmie", Warszawa 13 stycznia 2014 r .

Rozwój teleinformatyki i globalnego rynku automatyzuje procesy produkcyjne i finansowo–księgowe, umożliwia globalną i szybką komunikację, a nawet pozwala na zawieranie umów między kontrahentami na odległość (Rys. 2). Jednakże nie należy zapominać o tym, że prowadzenie działalności gospodarczej w oparciu o teleinformatyzację oprócz korzyści niesie za sobą różne zagrożenia. Systemy informatyczne stosowane w przedsiębiorstwach logistycznych mają na celu gromadzenie, przetwarzanie i szybkie udostępnianie danych, szczególnie o infrastrukturze krytycznej przedsiębiorstw logistycznych. Wielkość ich i jakość, a zwłaszcza źródło pochodzenia stanowią przedmiot zainteresowania nie tylko służb specjalnych i innych instytucji będących potencjalnym przeciwnikiem, ale także organizacji o charakterze terrorystycznym oraz pojedynczych osób. Systemy informatyczne mogą być zagrożone ze strony każdego, kto posiada dostateczny zasób wiedzy i umiejętności [9, s. 65].

Infrastruktura krytyczna przedsiębiorstw logistycznych ma oczywiście kluczowe znaczenie dla bezpieczeństwa państwa i obywateli, ale również w wymiarze bardziej lokalnym może mieć ogromne znaczenie dla bezpieczeństwa gospodarczego danej organizacji. W tym wymiarze pod uwagę brane są rozwiązania techniczne zapewniające działanie procesów w przedsiębiorstwie, przykładami takiej infrastruktury mogą być systemy: łączności, energetyczne, zarządzania dostępem, sterujące procesami produkcyjnymi, zapewniające odpowiednie warunki środowiskowe urządzeń i pomieszczeń, transportu wewnętrznego. Tak jak w każdym najlepiej nawet zabezpieczonym technicznie obiekcie, krytyczną

składową stanowi czynnik ludzki. Odpowiedni system rekrutacji i bieżącej kontroli personelu jest niezbędnym elementem każdego systemu bezpieczeństwa [3, s. 14].

5. ZARZĄDZANIE RYZYKIEM JAKO JEDEN Z NAJSKUTECZNIEJSZYCH SPOSÓB ZWIĘKSZENIA BEZPIECZEŃSTWA INFORMACJI

Użycie technologii informatycznych, do realizacji zadań biznesowych przedsiębiorstw logistycznych, jest zawsze obarczone pewnym ryzykiem, bywa, że maja one charakter losowy i niepowtarzalny. Taka sytuacja powoduje, że są one bardzo trudne do przewidzenia czy do powtórzenia w środowisku kontrolowanym, co więcej mogą one zależeć od wielu nieznanych dotychczas przyczyn. Mając na uwadze dobro przedsiębiorstwa, a co za tym idzie jego zysk w wymiarze ekonomicznym, nie możemy dopuścić do tego by szkodliwość negatywnych zjawisk wpłynęła na jakość procesów biznesowych. W tym rozumieniu ryzyko jest tym co powinniśmy starać się ograniczać, jednak aby było to możliwe musimy najpierw poznać poziom tego ryzyka, jego wpływ a także charakter.

Podstawą budowy i utrzymania systemu bezpieczeństwa informacyjnego przedsiębiorstwa jest właściwie ukierunkowany proces zarządzania ryzykiem, którego podstawowym zadaniem jest właśnie wspomniane ograniczanie [1, s. 74]. Warto tutaj wspomnieć że problematyka analizy ryzyka nie dotyczy jedynie dziedziny teleinformatyki. Wiele różnych dziedzin, dla których wpływ zdarzeń niepewnych może mieć negatywne skutki, zakłada potrzebę analizy ryzyka. W każdej z branż istnieje potrzeba analizy wpływu wielu powiązanych ze sobą i nierozpoznanych czynników na wystąpienie nieoczekiwanego zdarzenia, którego skutki czasem mogą być nawet katastrofalne. Trudno na przykład wyobrazić sobie aby firmy lotnicze produkujące samoloty nie przeprowadzały dogłębnej analizy ryzyka podczas wdrożenia nowych systemów informatycznych odpowiadających za sterowanie statkiem lotniczym.

Tak więc współcześnie możemy zauważyć wzrost znaczenia analiz ryzyka i ich coraz częstsze wykorzystywanie w celu zapewnienia bezpieczeństwa procesów oraz pracowników. Wzrost dokładności wykonywanych analiz, w późniejszych etapach może być wykorzystany do podejmowania kluczowych decyzji związanych ze skuteczniejszymi i tańszymi środkami redukcji zagrożeń. Analizy ryzyka wykonywane są w celach:

- Projektowych – identyfikacja i ocena potencjalnych zagrożenia w celu ich późniejszej eliminacji;
- Certyfikacyjnych – wydanie odpowiednich znaków bezpieczeństwa poświadczających właściwe warunki pracy urządzeń;
- Kierowania procesami – ogólna poprawa poziomu bezpieczeństwa, możliwość wypracowania skuteczniejszych procedur procesowych.

Analiza ryzyka składa się z kilku etapów [7, s. 221]. W pierwszym należy określić obszar dokonywanej analizy oraz jej kompleksowość. Jeśli źle określi się głębokość analizy, niektóre istotne elementy mogą zostać pominięte, co w konsekwencji doprowadzi do błędów w analizowaniu, a tym samym ograniczeniu jakości analizy. Druga faza analizy ryzyka polega na wykorzystaniu różnorodnych metod analitycznych. Można je podzielić na jakościowe i ilościowe, stosowane są w określonych celach i posiadają swoiste ograniczenia. W metodzie jakościowej ryzyko określa się jako niskie, średnie, wysokie, krytyczne. W metodzie ilościowej natomiast wyniki poziomu ryzyka określa się w konkretnych jednostkach miary, np. mnożnika prawdopodobieństwa jako wielkość kar umownych. Natomiast samo obliczanie ryzyka jest elementem trzeciej fazy analizy ryzyka. Niesie to ze sobą pewne komplikacje, ponieważ prawdopodobieństwo wystąpienia zdarzenia obliczane jest na podstawie danych niezawodności zdarzeń podstawowych. W celu określenia prawdopodobieństwa wystąpienia zdarzeń wykorzystuje się odpowiednie źródła informacji, są to:

- Dane statystyczne gromadzone przez samą organizację – w tym przypadku kluczowe znaczenie ma doświadczenie organizacji w danej branży;
- Dane statystyczne gromadzone przez inne organizacje ze zbliżonego sektora biznesowego, w tym jednak przypadku zachowuje się pewien poziom ostrożności;
- Szacowanie eksperckie – ich zaletą jest łatwa dostępność jednak bywają subiektywne;
- Szacowanie ekspercie korygowane różnymi metodami np. Delphi, co pozwala na zwiększenie prawdopodobieństwa i celności analizy.

Trzeba zwrócić uwagę na fakt, że poszczególne fazy analizy ryzyka wykorzystują pewne modele matematyczne, które symulują analizowane zjawiska. Wiąże się to z pewnymi ograniczeniami (chociażby mocą obliczeniową wykorzystywanych maszyn) i uproszczeniami.

Właściwe zdefiniowanie zagrożeń stanowi podstawę zapewnienia bezpieczeństwa informacji w przedsiębiorstwie. Zagrożenie to sytuacja lub stan, które komuś zagrażają lub w których ktoś czuje się zagrożony. Źródłem zagrożenia może być również osoba stanowiąca zagrożenie lub wzbudzająca poczucie zagrożenia.

Główne ryzyka związane z bezpieczeństwem informacji w przedsiębiorstwie definiujemy jako [9]:

- Ryzyko utraty poufności – zdarzenie mogące doprowadzić do ujawnienia informacji przetwarzanej przez system informatyczny nieautoryzowanemu użytkownikowi;
- Ryzyko utraty dostępności – zdarzenie mogące doprowadzić do braku dostępu w określonym czasie do systemu informatycznego, programu lub informacji dla autoryzowanych użytkowników;
- Ryzyko utraty integralności – zdarzenie mogące doprowadzić do nieautoryzowanej modyfikacji lub zniszczenia danych przetwarzanych przez systemy informatyczne.

WNIOSKI

W ramach przeanalizowanego materiału, dotyczącego zależności pomiędzy innowacyjnością przedsiębiorstw logistycznych a bezpieczeństwem przetwarzanych w nich danych, można wyróżnić kilka zasadniczych wniosków:

1. Innowacyjność przedsiębiorstw logistycznych jest niezbędnym czynnikiem ich rozwoju, a w dłuższej perspektywie czasowej determinuje ich przetrwanie na współczesnym konkurencyjnym rynku.
2. Informacja jest obecnie jednym z najcenniejszych wartości posiadanych przez firmy – jest ona towarem, a przez to jest ona również cennym narzędziem gospodarczym. Tak więc, informacja powinna być właściwie przetwarzana i chroniona przez dostępem osób niepożądanych.
3. Istnieje wiele standardów w zakresie utrzymania i rozwoju bezpieczeństwa informacji. Dzielą się one na oficjalne, czyli tworzone przez uznane gremia standaryzacyjne, np. ISO oraz na nieoficjalne, obejmujące zalecenia różnych organizacji, firm i stowarzyszeń.
4. Najbardziej istotą kwestią wpływającą na poziom bezpieczeństwa systemów informatycznych jest aktualność i kompletność bazy zdefiniowanych błędów. Do najczęstszych błędów popełnianych przez firmy w tym zakresie należą: luki w zabezpieczeniach, przestarzałe oprogramowanie zabezpieczające, brak wiedzy lub zaangażowania w dostosowanie systemów monitorujących lub skanerów, słabe hasła szyfrujące lub ich udostęp-

nianie. Aby zapobiegać tego typu błędom należy przede wszystkim zadbać o edukację personelu, gdyż jak wynika z wielu badań, człowiek jest najsłabszym ogniwem we wszelkich systemach bezpieczeństwa.

5. Z punktu widzenia przedsiębiorstwa logistycznego, dla którego informacja może być znaczącym determinantem wpływającym na jego konkurencyjność, informacja powinna być: kompletna, istotna, terminowa, właściwa, wiarygodna, zrozumiała. Wszelkie zasoby informacje przedsiębiorstw są obecnie gromadzone, przetwarzane i udostępniane głównie poprzez systemy informatyczne. Należy pamiętać, że mogą one stanowić przedmiot zainteresowania nie tylko innych podmiotów gospodarczych, ale i służb specjalnych, a także organizacji o charakterze terrorystycznym.
6. Podstawą budowy i utrzymania systemu bezpieczeństwa informacyjnego przedsiębiorstwa jest właściwie ukierunkowany proces zarządzania ryzykiem, który realizuje się na potrzeby projektowania, certyfikowania i kierowania procesami informacyjnymi. Analizując ryzyko wykorzystuje się szereg statystycznych danych historycznych, ale i szacowanie eksperckie oraz inne metody jakościowe i ilościowe.

BIBLIOGRAFIA

1. Białas A., Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, Warszawa, 2007.
2. Kuta M., Polityka bezpieczeństwa informacji w przedsiębiorstwie – aspekty praktyczne, [w:] Borowiecki R., Kwieciński M., Monitorowanie otoczenia, przepływ i bezpieczeństwo informacji. W stronę integralności przedsiębiorstwa, Zakamycze 2003.
3. Kopczewski M., Elementy infrastruktury krytycznej państwa (organizacji) – jako obiekty narażone na ataki cyberterrorystyczne, Poznań 2014.
4. Kopczewski M., Tobolski M., Information security as an element of securitybstrategy of a company, [w]: Innowacje w zarządzaniu i inżynierii produkcji, tom I, Opole 2015.
5. Liedel K., Bezpieczeństwo informacyjne, 2008, dostęp w dn. 28.08.2015 r. z: http://www.liedel.pl/?p=13.
6. Łuczak J. (red.), Zarządzanie bezpieczeństwem informacji, Oficyna Współczesna, Poznań 2004.
7. Markowski A. S., Zapobieganie stratom w przemyśle, Cześć III - Zarządzanie bezpieczeństwem procesowym, Łódź 2000.
8. PN-I-I3335-1: Technika Informatyczna – wytyczne do zarządzania bezpieczeństwem systemów informatycznych, PKN, 1999 oraz PN-I-I3335-2: Technika informatyczna: Planowanie i zarządzanie bezpieczeństwem systemów informatycznych, PKN, 2003.
9. Żebrowski A., Kwiatkowski M., Bezpieczeństwo informacji III Rzeczypospolitej, Oficyna Wydawnicza Abrys, Kraków 2000.

INNOVATION OF LOGISTICS COMPANIES IN RELATION TO INFORMATION SECURITY

Abstract

The aim of the article is to present the problems associated with management of information and searching for balanced relationship and an appropriate balance between the development of innovation, logistics companies and security they process information. Information, as one of the most valuable corporate resources, should be the object of particular concern. Therefore, this article discusses such issues connected with management of information as: the role of information management, including components of an information system, normalization and standardization of the analyzed processes, information security - its components and the organization and management of risk in the system of information security. The analyzed materials helped to conclude the most important issues related to information security in relation to the operation and development of logistic companies.

Autorzy:
dr hab. inż. Tomasz Smal, prof. WSOWL - Wydział Nauk o Bezpieczeństwie, Wyższa Szkoła Oficerska Wojsk Lądowych imienia generała Tadeusza Kościuszki we Wrocławiu, +48 261 658 330, t.smal@wso.wroc.pl.
prof. dr hab. inż. Marian Kopczewski - Wydział Nauk o Bezpieczeństwie, Wyższa Szkoła Oficerska Wojsk Lądowych imienia generała Tadeusza Kościuszki we Wrocławiu, m.kopczewski@wso.wroc.pl.