PAŁĘGA Michał [1]

Analiza technicznych i organizacyjnych środków bezpieczeństwa informacji na przykładzie przedsiębiorstwa logistycznego

WSTĘP

Logistyka w swojej istocie trudni się planowaniem, realizowaniem oraz kontrolowaniem sprawnego i efektywnego pod względem ekonomicznym przepływu surowców, materiałów, wyrobów gotowych, a także odpowiedniej informacji z punktu pochodzenia do punktu konsumpcji w celu zaspokojenia potrzeb odbiorców[4]. Zatem można założyć, iż dobra informacyjne mają ogromne znaczenie w procesach logistycznych wpływając na jakość tychże procesów, a w konsekwencji generując wartość dodaną dla klienta.

Podmioty gospodarcze działające w sektorze usług logistycznych, jak również działy logistyki w przedsiębiorstwach o profilu produkcyjnym czy handlowym bazują na ogromnym przepływie informacji i danych. Jako przykład można wskazać chociażby informacje o produktach, dla których ustala się plany produkcji, surowcach czy materiałach niezbędnych do ich wytworzenia, czy też informacje dotyczące realizacji zamówień i obsługi klienta. Z funkcjonalnego punktu wiedzenia w całym systemie logistycznym można wskazać następujące kategorie informacji[4]:

1. Informacje twarde – dokumenty papierowe (listy przewozowe, dokumenty magazynowe itp.);
2. Informacje związane z produktem – naklejki adresowe, produktowe, logistyczne (np. opakowaniowe);
3. Informacje związane z obsługą procesu – zlecenia, potwierdzenia (elektroniczne, papierowe, ustne);
4. Informacje związane z finansami – dokumenty księgujące proces (np. faktury),
5. Informacje związane z przepływem materiałowym – elektroniczne pliki danych, polecenia technologiczne (np. polecenie pobrania w procesie kompletacji, które może być głosowe, świetlne, papierowe lub na skanerze);
6. Informacje ogólne i pomocnicze dla realizacji procesu.

Wobec powyższego nieodzownym elementem funkcjonowania firm logistycznych są systemy informatyczne. Do wymiernych korzyści płynących z ich zastosowania można zaliczyć sprawny przepływ towarów, minimalizację powierzchni magazynowych, zoptymalizowane prognozowanie i planowanie przepływów i środków transportu, a także sprawny obieg dokumentów. Zakłada się, że rynek aplikacji magazynowych i logistycznych jest jedną z prężniej rozwijających się dziedzin w branży IT[11,14].

Jak wskazano powyżej rozwiązania informatyczne są współcześnie motorem napędowym każdego przedsiębiorstwa, z kolei w przypadku podmiotów logistycznych ich rola jest znacznie większa, gdyż nie mogą one istnieć i działać poprawnie bez odpowiednich systemów informatycznych. Niezmiernie istotnym aspektem jest posiadanie takiego systemu, który sprosta rosnącej fali włamań i ataków komputerowych, będzie odporny na uszkodzenia oraz wyposażony w mechanizmy gwarantujące bezpieczeństwo przechowywanych i przetwarzanych w nim danych[9].

Celem artykułu jest wskazanie istoty bezpieczeństwa informacji w przedsiębiorstwie usług logistycznych, analiza i ocena zagrożeń ze szczególnym uwzględnieniem podatności na jakie narażone są dobra informacyjne gromadzone, przetwarzane i transmitowane za pośrednictwem sieci teleinformatycznej. Ponadto w artykule dokonano charakterystyki wybranych rozwiązań technicznych i organizacyjnych gwarantujących racjonalny poziom bezpieczeństwa danych.

[1] Politechnika Częstochowska, Al. Armii Krajowej 36, 42-200 Częstochowa, e-mail: mpalega@wip.pcz.pl

1. IDEA BEZPIECZEŃSTWA INFORMACJI

W świecie zdominowanym przez różnego typu zagrożenia takie jak: katastrofy naturalne i ekologiczne, działalność terrorystyczna, militarna i polityczna, kryzysy ekonomiczne i społeczne oraz wiele innych – bezpieczeństwo traktowane jest w kategorii jednej z najcenniejszych wartości dla państwa, podmiotów gospodarczych, instytucji rządowych oraz pojedynczych jednostek społecznych. Wobec tego bezpieczeństwo (w tym również bezpieczeństwo zasobów materialnych i niematerialnych) powinno stanowić kluczowy obszar zainteresowań w zarządzaniu organizacją – niezależnie od formy jej zorganizowania, szczebla hierarchicznego czy stopnia rozwoju[7].

Jak zaznaczono we wstępie, informacje to jedne z najważniejszych dóbr jakim dysponują bądź chciałby dysponować przedsiębiorstwa. Pokreślić należy, że jedne z nich mogą mieć mniejsze znaczenie dla organizacji oraz jej wewnętrznego i zewnętrznego otoczenia, inne zaś wręcz przeciwnie – mogą pełnić strategiczną rolę w realizacji wyznaczonej przez podmioty misji i związanych z nią celów i zadań. To właśnie te informacje wymagają należytej ochrony. Dlatego też zagwarantowanie bezpieczeństwa informacji stanowi podstawowe zadanie, a jednocześnie wyzwanie każdego współczesnego podmiotu gospodarczego czy instytucji.

Bezpieczeństwo informacji jest złożonym zagadnieniem o charakterze interdyscyplinarnym, obejmującym swoim zasięgiem kwestie dotyczące przede wszystkim[6,7]:

- samej informacji, jej istoty, specyficznej postaci oraz często niejasnych i niezrozumiałych dla wielu osób treści (pracownicy nie są świadomi ukrytej wartości informacji mylnie postrzeganych przez nich za nieszkodliwą);
- systemów, w których są wytwarzane, przetwarzane, przechowywane oraz dystrybuowane dane;
- środowiska, w których działają te systemy; ocena zagrożeń bezpieczeństwa informacji powinna dotyczyć m.in. pomieszczenia, okablowania, czy zasilania;
- personelu, który jest użytkowaniem tychże systemów; jego niefrasobliwość i nieobliczalność często stanowi o porażce systemu bezpieczeństwa informacji;
- zgodności z polskimi oraz europejskimi wymogami prawnymi.

Bezpieczeństwo informacji to szereg działań zintegrowanych na nieustanne doskonalenie mechanizmów gwarantujących im ochronę przed nieuprawnionym dostępem, zniszczeniem bądź ujawnieniem. W konsekwencji oznacza zatem zachowanie podstawowych atrybutów: poufności, integralności i dostępności, które zgodnie z międzynarodowym standardem ISO/IEC 27001:2007 definiowane są w następujący sposób:

- POUFNOŚĆ – właściwość polegająca na tym, że informacje nie są udostępniane lub ujawniane osobom bądź podmiotom do tego nieupoważnionym;
- INTEGEALNOŚĆ – właściwość polegająca na tym, że informacje są dokładne, kompletne, niezmodyfikowane;
- DOSTĘPNOŚĆ – właściwość polegająca na tym, że informacje są dostępne oraz użyteczne na każde żądanie uprawnionego podmiotu, w odpowiednim czasie i miejscu.

Bezpieczeństwo aktywów informacyjnych osiąga się poprzez zastosowanie kombinacji przedsięwzięć obejmujących środki fizyczne, organizacyjne, osobowe oraz techniczne. Wdrażając odpowiedni zestaw zabezpieczeń należy zadbać o to, aby były one zgodne z poszczególnymi celami bezpieczeństwa oraz prowadzoną działalnością gospodarczą. Ważne jest również to, aby zastosowane zabezpieczenia nie były nazbyt uciążliwe dla jego użytkowników, gdyż w przeciwnym razie istnieje ryzyko, iż będą one omijane przez pracowników, co w konsekwencji zdecyduje o ich nieskuteczności, a incydenty związane z wyciekiem informacji będą jedynie kwestą czasu. Pamiętać należy przy tym, iż zapewnienie właściwej ochrony informacji powinno stanowić ciągły i systematyczny proces. Postępujący rozwój cywilizacyjny i technologiczny sprzyja powstawaniu coraz to nowszych form zagrożeń oraz eskalacji już istniejących, w tym także dotyczących sfery informacyjnej wobec których organizacje muszą skutecznie stawiać czoła. Dlatego też jednym z priorytetów każdej organizacji powinna być troska o zachowanie bezpieczeństwa przejawiająca się m.in. w: identyfikacji zagrożeń zarówno tych bieżących, jak i potencjalnych (mogących wystąpić w przyszłości), permanentnej

analizie i ocenie podatności zasobów, czyli luk i braków pojawiających się w systemie zabezpieczeń oraz ciągłym doskonaleniu mechanizmów obronnych.

2. IDENTYFIKACJA ZAGROŻEŃ

Zagrożenia stanowić mogą potencjalną przyczynę niepożądanego incydentu wywołującą szkodę dla systemu bądź organizacji i jej zasobów. Szkoda ta może powstać w wyniku bezpośredniego bądź pośredniego ataku na informację przetwarzaną przez system lub usługę informatyczną, co w konsekwencji może prowadzić do jej uszkodzenia, ujawnienia osobom czy jednostkom nieupoważnionym do ich dostępu, modyfikacji, a niekiedy nawet całkowitej jej utraty[10].

Identyfikacja i ocena zagrożeń powinna uwzględniać zagrożenia wewnętrzne i zewnętrzne oraz zagrożenia wynikające ze zdarzeń losowych. Zagrożenia wewnętrzne dotyczyć mogą sprzętu komputerowego, oprogramowania oraz ludzi (pracowników organizacji). Z kolei zagrożenia zewnętrzne płyną z otoczenia przedsiębiorstwa i zazwyczaj związane są ze specyfiką działalności podmiotu gospodarczego oraz wykorzystywaniem sieci Internet[6].

Zgodnie z ww. kryterium zagrożenia związane z bezpieczeństwem informacji można skategoryzować następująco[6]:

1. Zagrożenia fizyczne:
– kradzież lub fałszowanie informacji
– kradzież sprzętu lub nośników danych
– celowe niszczenie
– wandalizm lub ataki cyberprzestępców
– oszustwa komputerowe
2. Zagrożenia technologiczne:
– awaria sprzętu komputerowego
– awarie systemowe oraz błędy programów
– blokady działania systemów przez zawirusowanie lub wywołanie przeciążeń
3. Zagrożenia związane z transmisją danych:
– celowy podsłuch
– nieautoryzowany dostęp do systemu
4. Zagrożenia ze strony użytkowników:
– błędy i pomyłki użytkowników
– akty zemsty byłych lub zatrudnionych pracowników
– wykorzystanie sprzętu lub oprogramowanie do celów prywatnych
5. Zdarzenia losowe:
– żywioły: ogień, woda, pioruny.

W czasach powszechnej dostępności do Internetu szczególnego znaczenia nabierają zagrożenia płynące z sieci komputerowej, które są niezwykle złożone, a co trzeba również podkreślić często niestety lekceważone. Do najbardziej popularnych zalicza się[5,15]:

– *wirusy komputerowe* (ang. computer virus) – złośliwe programy samo replikujące, mające za zadanie umieścić własny kod w określonym miejscu na dysku lub w programie, a tym samym zniszczyć zapisane na dyskach informacje;
– *włamania* – wykorzystanie „dziur oprogramowania" celem przejęcie kontroli nad niezabezpieczonymi komputerami;
– *konie trojańskie* (ang. Trojan house) – programy „udające" ciekawe i interesujące aplikacje, w których zaszyta jest dodatkowa funkcjonalność umożliwiająca przejęcie kontroli nad komputerem bez wiedzy jego właściciela, np. przechwytywanie znaków wprowadzanych na klawiaturze;
– *ataki typu exploit* – ataki (lub narzędzia) wykorzystujące błąd lub lukę aplikacji bądź systemu operacyjnego najczęściej do przepełniania buforów i umieszczania podprogramów w losowych miejscach w pamięci normalnie zabronionych przez użytkownika;

- DoS - odmowa wykonania usługi; ataki typu exploit polegające na tym, że zaatakowany komputer nie jest w stanie zagwarantować poprawnej realizacji pojedynczej usługi bądź całego serwera; ataki DoS nigdy nie prowadzą do wykradania danych, a raczej uniemożliwiają do nich dostęp oraz realizację świadczonych usług;
- keyllogery – programy (rzadziej urządzenia) rejestrujące klawisze naciskane przez użytkownika;
- spyware – programy szpiegujące; gromadzą informacje o użytkowniku systemu oraz wysyłają je autorowi oprogramowania;
- phishing – bardzo poważna i groźna odmiana spamu polegająca na tworzeniu fałszywych wiadomości e-mail i stron WWW wyglądających identycznie z oryginalnymi stronami instytucji finansowych, aukcji i sklepów internetowych; wykorzystywane są do wyłudzenia haseł logowania, numerów kart kredytowych czy informacji dotyczących kont bankowych;
- farming (ang. pharming) – skierowanie użytkownika na fałszywą stronę WWW (wyglądającą tak samo jak prawdziwa) celem wyłudzenie jego poufnych danych, np. odnośnie konta bankowego;
- spoofing – podszywanie się pod inny komputer w sieci;
- hijacking – ataki polegające na przechwytywaniu połączeń między komputerami – przechwytywanie sesji;
- sniffing – programy komputerowe bądź urządzenia przeznaczone do przechwytywania danych przesyłanych w sieci i późniejszego ich analizowania.

Szczególnego rodzaju zagrożeniem jest socjotechnika, określana również jako inżynieria społeczna, która bazuje m.in. na naiwności, niefrasobliwości oraz braku dostatecznej wiedzy człowieka w celu uzyskania pożądanych informacji. Jest to bardzo skuteczna technika, jeśli chodzi o dostęp do danych wrażliwych, np. odbiorców, haseł systemowych itp. Dostępna literatura przedmiotu wskazuje na najbardziej typowe metody socjotechniczne, do których zaliczyć można:

- udawanie pracownika tej samej organizacji;
- udawanie przedstawiciela dostawcy, firmy partnerskiej lub agencji rządowej;
- udawanie kogoś, kto ma władzę;
- udawanie nowego pracownika, potrzebującego pomocy;
- wysyłanie darmowego programu do aktualizacji lub zainstalowania;
- wysyłanie wirusa lub konia trojańskiego w załączniku do poczty e-mail;
- przechwytywanie naciśniętych klawiszy (np. haseł) za pomocą specjalnego oprogramowania;
- podrzucanie mobilnych nośników danych w miejsce stanowiska pracy ofiary zawierających niebezpieczny kod;
- oraz wiele pokrewnych metody oddziałujących na emocje jednostki społecznej.

3. SYSTEM ZABEZPIECZEŃ

W najprostszym ujęciu zabezpieczenia to wszelkiego rodzaju praktyki, procedury oraz mechanizmy redukujące ryzyko związane z nieupoważnionym dostępem do informacji, ich modyfikacją, zniszczeniem czy całkowitą utratą. Efektywna ochrona wymaga zazwyczaj zaimplementowania zabezpieczeń technicznych w kombinacji z procedurami bezpieczeństwa określającymi podstawowe reguły zachowania i postępowania pracowników organizacji. Do podstawowych funkcji zabezpieczeń zalicza się:[3]

- ochronę przed zagrożeniami;
- odstraszanie intruzów;
- redukcję wpływu podatności;
- ograniczanie następstw;
- wykrywanie incydentów bezpieczeństwa oraz zapobieganie im;
- ułatwianie odtworzenia naruszanych zasobów.

Pozostałe, wspomagające funkcje zabezpieczeń to:[3]

- uświadamianie;
- szkolenie;

– monitorowanie;
– działania naprawcze i korygujące.

W dalszej części niniejszego opracowania zaprezentowanych zostanie kilka przykładowych rozwiązań technicznych i organizacyjnych, jakie mogą zostać zaimplementowane przez przedsiębiorstwa logistyczne w celu ochrony zasób informacyjnych, a w szczególności tych gromadzonych i przetwarzanych w systemach informatycznych.

3.1. Zabezpieczenia techniczne

Kontrola dostępu

Kontrola dostępu to system wzajemnie powiązanych urządzeń oraz wdrożonych procedur organizacyjnych nakładający mechanizmy restrykcji dostępu do pomieszczeń (np. serwerownia), jak również systemu komputerowego lub jego części stosowany w celu ochrony znajdujących się w nim zasobów. Ochrona ta realizowana jest poprzez całkowite uniemożliwienie dostępu do pomieszczeń chronionych osobom nieupoważnionym lub czasowe ograniczenie dostępu osobom posiadającym uprawnienie do wejścia w ściśle określonym czasie (dzień tygodnia, godzina). Kontrola dostępu do informacji i systemów komputerowych najczęściej wiąże się z procesem uwierzytelniania polegająca na podaniu właściwego identyfikatora (login-u) oraz przypisanego do niego hasła. Kontrola dostępu poprzez uwierzytelnienie pozwala na[12]:

– zapobieganie nieuprawnionemu dostępowi do sprzętu komputerowego;
– zapobieganie nieuprawnionemu dostępowi użytkowników;
– zagwarantowanie ochrony usług sieciowych;
– zapobieganie nieuprawnionemu dostępowi do danych przechowywanych zarówno w formie tradycyjnej jak również w systemach informatycznych;
– wykrywanie nieuprawnionej aktywności.

Wśród najbardziej popularnych metod uwierzytelniania można wskazać następujące[8,14]:

a) hasła – czyli krótkie sekwencje liter, cyfry i innych znaków; polityka bezpieczeństwa podkreśla, że powinny one być odpowiednio „silne" w zależności od zasobów, do jakich pozwalają dostać się ich użytkownikom. Nie powinno się stosować haseł, które wynikają z nazwy jego użytkownika itp. Bezpieczne hasło powinno zawierać małe i duże litery, cyfry oraz znaki specjalne. Doskonałym rozwiązaniem może być zastosowanie odpowiedniego oprogramowania, które będzie uniemożliwiało generowanie zbyt słabych haseł. Ponadto, zaleca się częstą zmianę haseł oraz jego blokowanie po trzech nieudanych próbach jego użycia. Ważnym aspektem polityki haseł jest ich przechowywanie w miejscach niedostępnych dla osób niepowołanych. Doświadczenia dnia codziennego pokazują, iż wiele osób przykleja karteczki z hasłem do monitorów komputerów bądź umieszcza je pod klawiaturą. W przypadkach takich hasła tracą swoją funkcję zabezpieczającą oraz powodują złudne poczucie bezpieczeństwa.

b) inteligentne karty – działają w oparciu o kryptograficzny protokół uwierzytelniania (typu wezwanie – odpowiedź). Zasada ich działania jest następująca – system generuje pewną losową liczbę i podaje ją użytkownikowi, następnie ten wprowadza ją do karty, która szyfruje liczbę. Wynik szyfrowania zwracany jest do systemu, który weryfikuje poprawność szyfrowania. Tego rodzaju karty wykorzystywane są do logowania w sieci, na komputerze lub urządzeniu.

c) techniki biometryczne – wykorzystują indywidualne cechy fizyczne lub behawiorystyczne człowieka do jego identyfikacji bądź potwierdzenia tożsamości. Do cech fizycznych zalicza się m.in.: linie papilarne, geometrię dłoni, tęczówkę i siatkówkę oka, charakterystykę twarzy. Z kolei cechy behawiorystyczne (związane z zachowaniem) tworzą: styl chodu, podpisu, pisania na klawiaturze czy głos.

Kryptografia

Popularność Internetu powoduje, że podstawowym medium komunikacji przedsiębiorstwa z jego klientami, dostawcami, usługodawcami czy też innymi podmiotami gospodarczymi stanowi poczta elektroniczna. Nastręcza to konieczność należytego poziomu bezpieczeństwa informacji przesyłanych za jej pośrednictwem. W celu zagwarantowania poufności danych przesyłanych pocztą elektroniczną

wykorzystuje się techniki kryptograficzne (szyfrowanie). Proces ten polega na transformacji oryginalnego tekstu na ciąg znaków pozornie nic nie znaczących dla osoby postronnej, którego odczytanie wymaga znajomości odpowiedniego klucza. Należy podkreślić, iż występuje następująca zależność: im większa liczba cyfr tworzących długość klucza, tym większe bezpieczeństwo, że atakujący nie odkryje kombinacji cyfr i nie odszyfruje oryginalnej wiadomości. Aktualnie stosuje się dwie metody szyfrowania przesyłanych danych: szyfrowanie z kluczem symetrycznym oraz szyfrowanie z kluczem asymetrycznym. Szyfrowanie z kluczem symetrycznym zakłada wykorzystanie tego samego klucza zarówno przez nadawcę wiadomości do jej zaszyfrowania, jak również przez odbiorcę do jej deszyfrowania i odczytania właściwej zawartości pliku. Szyfrowanie z kluczem asymetrycznym wymaga zastosowania dwóch skorelowanych ze sobą kluczy – klucza publicznego i klucza prywatnego. Z klucza publicznego korzysta nadawca wiadomości do jej utajnienia, z kolei odbiorca do oczytania jej zawartości musi zastosować klucz prywatny[1].

System wykrywania włamań IDS

System IDS stanowią urządzenia sieciowe, które poprzez wykrywanie włamań w czasie rzeczywistym zwiększają poziom bezpieczeństwa sieci komputerowych. Na podstawie analizy ruchu sieciowego identyfikują podejrzane działanie naruszające zasady polityki bezpieczeństwa danych w systemie, jak np. próby penetracji, włamań czy ataki intruzów. Zasadniczymi zadaniami systemu wykrywania włamań ISD jest detekcja wzorów nadużyć bazując na wiedzy o nienormalnych zachowaniach lub sygnaturach ataków oraz rozpoznawanie anomalii, czyli odmiennych zachowań w oparciu o profil normalnego zachowania użytkowników i systemu[1,8].

Firewall

Zapora sieciowa (firewall) to kolejny mechanizm zabezpieczający dane zgromadzone w systemie przez intruzami. Zaporę sieciową mogą tworzyć zarówno sprzęt komputerowy z dedykowanym oprogramowaniem, jak również samo oprogramowanie blokujące dostęp do komputera nieupoważnionego użytkownika. Zapora sieciowa zapewnia bezpieczeństwo pracy w sieci lokalnej i Internecie. Wyróżnia się trzy podstawowe typu zapór sieciowych[8]:

- filtrujące – monitorują przepływające przezeń pakiety sieciowe i przepuszczają tylko zgodne z regułami ustawionymi na danej zaporze (zapora pracująca dodatkowo jako router). Zwykle zapora sprzętowa bądź dedykowany komputer z systemem operacyjnym Linux.
- translacja adresów sieciowych (NAT) – bazuje na zmianie adresu IP hosta wewnętrznego w celu ukrycia go przed zewnętrznym monitorowaniem.
- zapory pośredniczące (proxy): wykonujące połączenie w imieniu użytkownika.

Zapory sieciowe są jednym z najskuteczniejszych mechanizmów ochrony przed nieuprawnionym dostępem do sieci. Należy jednak pamiętać, iż przy całym swoim dobrodziejstwie ten rodzaj zabezpieczenia nie uchroni zasobów informacyjnych przedsiębiorstwa przed ludzką naiwnością i nieuczciwością czy brakiem dostatecznej wiedzy użytkowników systemu.

3.2. Zabezpieczenia organizacyjne

Zabezpieczenia organizacyjne tworzy grupa środków ochronny stosowanych w procesach informacyjnych. Składają się na nie różnorodne techniki i metody, które bezpośrednio dotyczą procesu zarządzania bezpieczeństwem informacji. Wyodrębnić w nich należy szczególną grupę zabezpieczeń – zabezpieczenia kadrowe. Podstawową ich rolą jest minimalizacja ryzyka utraty poufności informacji na skutek błędu pracownika, jego niekompetencji, nieuczciwego działania, oszusta czy nadużycia uprawnień. Zabezpieczenia organizacyjne wpływają również pozytywnie na budowanie świadomości użytkowników w zakresie zagrożeń związanych z bezpieczeństwem informacji[2].

Przedsiębiorstwa chcące stworzyć w miarę skuteczny system bezpieczeństwa informacji powinny skupić się na następujących działaniach[9]:

Po pierwsze – niezbędne jest odpowiednie zorganizowanie procesów pracy, łącznie z precyzyjnym wyznaczeniem kompetencji pracowników oraz ich wzajemnych zależności i powiązań. Jest to na tyle istotne, gdyż wiele poufnych informacji wydostaje się poza obszar organizacji na skutek braku

dostatecznej wiedzy pracowników oraz przekraczania przez nich uprawnień. Remedium na tego typu sytuacje jest ograniczenie nadawanych do systemu uprawnień użytkownikom zgodnych z zakresem działań realizowanych na konkretnym stanowisku pracy.

Po drugie – należy stworzyć procedury dostępu do poszczególnych budynków i pomieszczeń osobom postronnym np. sprzątającym biuro, serwisantom czy monterom instalującym nowe urządzania.

Po trzecie – ważną częścią systemu bezpieczeństwa informacji w przedsiębiorstwie jest również opracowanie zasad określających dostęp do budynków i pomieszczeń w przypadku wystąpienia zdarzeń nagłych, jak np. pożar.

Po czwarte – istotną kwestią jest ograniczenie obiegu dokumentów między działami oraz określenie sposobów ich cyrkulacji w firmie. Bardzo często dokumenty z poufnymi informacji krążą z pokoju do pokoju w poszukiwaniu właściwego ich adresata. Zagrożenia jakie się z tym wiążą to przede wszystkim dostęp do informacji osobom nieupoważnionym, ryzyko zgubienia dokumentów bądź ich zniszczenia.

Po piąte – zasadniczym jest utworzenie precyzyjnych i zrozumiałych regulaminów i procedur pracy. Pracownicy powinni zostać zobligowani między innymi do przestrzegania zasad polityki czystego biurka i ekranu, polityki korzystania ze służbowego sprzętu komputerowego, poczty elektronicznej i innych powierzonych im zasobów (jednie do celów prywatnych), podczas chwilowej nieobecności stosowania wygaszacza ekranu z hasłem itp. Należy zaznaczyć, iż wiele zagrożeń związanych z utratą poufności danych wynika właśnie z łamania przez pracowników wymienionych zasad bezpieczeństwa.

Po szóste – organizacje muszą zadbać o systematyczne szkolenie personelu oraz budowanie wśród nich świadomości odpowiedzialności za bezpieczeństwo danych i informacji w przedsiębiorstwie. W sytuacji, gdy jednie zostaną spisane reguły i praktyki bezpieczeństwa, a pracownicy zostaną z nimi pobieżnie zapoznani i zobowiążą się do ich przestrzegania nie można mówić o skutecznej organizacji systemu bezpieczeństwa informacji. Szczególnie ważne, w tym przypadku jest wskazanie pracownikom celowości stosowanych zabezpieczeń. Wszyscy zatrudnieni muszą być świadomi czyhających zagrożeń, a w razie ich wystąpienia potrafić je właściwie i szybko zidentyfikować oraz podjąć właściwe kroki ograniczające skutki ich zaistnienia.

Po siódme – niezbędne jest także zapoznanie pracowników z restrykcjami i konsekwencjami za naruszanie zasad bezpieczeństwa informacji w przedsiębiorstwie. Wszystkie incydenty związane z nieprzestrzeganiem przyjętych praktyk bezpieczeństwa nie mogą być tolerowane i pobłażane. Niemniej jednak ważną rolę w systemie bezpieczeństwa informacji pełni właściwa motywacja pracowników oraz ich nagradzanie, np. za udaremnienie ataku intruza.

Polityka bezpieczeństwa zasobów informatycznych

Polityka bezpieczeństwa stanowi zbiór zasad, jakich muszą przestrzegać użytkownicy w celu zapewnienia zachowania integralności gromadzonych i przetwarzanych przez system danych. Jej istotą jest przeciwdziałać zagrożeniom, na jakie narażone są zasoby informatyczne. Mogą one wynikać z[13]:

- braku świadomości zagrożeń;
- nadmiernych kosztów wdrażania zabezpieczeń;
- omijania złożonych, często utrudniających codzienną pracę procedur uwierzytelniania czy autoryzacji;
- braku współpracy użytkowników, służb informatycznych oraz producentów systemów zabezpieczeń.

Polityka zabezpieczeń powinna występować w postaci jawnego dokumentu, a jej zapisy być zgodne i niesprzeczne z wewnętrznymi celami i zadaniami organizacji oraz definiować w sposób jasny i zrozumiały zakres czynności i obowiązków użytkowników systemu informacyjnego. W dokumencie tym należy uwzględnić następujące zasady[13]:

Jednostkowej odpowiedzialności – każdy zbór danych w systemie powinien mieć swojego właściciela, który będzie za niego odpowiedzialny;

Wiedzy koniecznej – każdy użytkownik systemu powinien mieć nadane uprawnia dostępu do systemu zgodnie z zakresem jego obowiązków;
Obecności koniecznej – w pomieszczeniach powinni przebywać jednie uprawnieni pracownicy – wykonujący swoje obowiązki służbowe; wyklucza się zatem pracowników oraz osoby z zewnątrz nie mające związku z obowiązkami służbowymi;
Wieloosobowej organizacji – funkcje, które mogą osłabić bądź złamać system ochrony powinny być realizowane przynajmniej przez dwie osoby;
Rotacji pracowników – funkcje wiążące się z dostępem do szczególnie poufnych danych powinny być przydzielane okresowo;
Oddzielania przywilejów – dostęp do zasobu powinien wiązać się ze spełnieniem więcej niż jednego warunku;
Najmniejszego wspólnego środka bezpieczeństwa – liczba osób korzystających ze wspólnego środka bezpieczeństwa powinna być możliwie jak najmniejsza, np. hasła powinny być przypisywane tylko jednemu użytkownikowi systemu bądź aplikacji;
Psychicznej akceptowalności – użytkowanie systemów zabezpieczeń nie powinno sprawiać nadmiernych trudności pracownikom;
Całkowitego pośrednictwa – dostęp do zasobu powinien zostać poprzedzony procesem weryfikacji tożsamości potencjalnego użytkownika.

PODSUMOWANIE

Działalność na rynku usług logistycznych w dużym stopniu determinowana jest posiadanymi dobrami informacyjnymi. Są one zbierane, gromadzone, przetwarzane oraz transmitowane wewnątrz i na zewnątrz organizacji. Wielokrotnie poddaje się je również różnego typu analizom. Popularność stosowanych systemów informatycznych wspomagających tworzenie raportów dotyczących niemalże wszystkich sfer działalności przedsiębiorstwa powoduje znaczny wzrost ilości produkowanych informacji niż było to kilkanaście lat temu. Na tej płaszczyźnie powstaje bardzo wiele zagrożeń determinujących utratę poufności, integralności i dostępności danych. Wobec powyższego organizacje zobligowane są do tworzenia bezpiecznych warunków związanych z ich przechowywaniem oraz użytkowaniem.

W czasach powszechnej informatyzacji społeczeństwa szczególnego znaczenia nabiera bezpieczeństwo systemów informatycznych, które coraz trudniej osiągnąć głównie za sprawą pracy w globalnej sieci Internet. Z jednej strony pozwalają one na szybką i efektywną obsługę klienta, z drugiej zaś wymagają implementacji coraz to bardziej zaawansowanych technologicznie i kapitałochłonnych zabezpieczeń. Bezpieczeństwo systemów informatycznych i zawartych w nich danych wiąże się także z opracowaniem, wdrożeniem, przestrzeganiem oraz ciągłym udoskonalaniem własnej polityki bezpieczeństwa, pozwalającej utrzymać ustalony poziom poufności, integralności, dostępności i niezawodności.

Reasumując praktyczne zastosowanie polityki bezpieczeństwa musi opierać się na jej ludzkim oraz technicznym wymiarze, stąd też zabezpieczenia technicznie w połączeniu z rozwiązaniami organizacyjnymi daje realne szanse na unikniecie kompromitacji systemu bezpieczeństwa informacji w przedsiębiorstwie.

Streszczenie

Informacja i technologia informacyjna pełnią istotną rolę w działalności logistycznej oraz mają coraz większy wpływ na sukces rynkowy organizacji i utrzymanie jej konkurencyjności. Nieprzerwany przepływ zasobów informacyjnych stanowi podstawę efektywnego funkcjonowania łańcucha dostaw. Zasoby informacyjne narażone są na różnego rodzaju ryzyka, które mogą doprowadzać do powstawania znaczących start i szkód. Dlatego też bezpieczeństwo informacji trzeba traktować jako kluczowy element procesu zarządzania przedsiębiorstwem logistycznym.

W artykule przedstawiono identyfikację zagrożeń wpływających na poziom bezpieczeństwa informacji w przedsiębiorstwie. Ponadto, dokonano analizy zabezpieczeń technicznych oraz rozwiązań organizacyjnych, gwarantujących ochronę informacji przed zagrożeniami. Brak tego typu zabezpieczeń w organizacji generuje powstawanie zdarzeń związanych z utratą, modyfikacją bądź nieautoryzowanym dostępem do danych firmy.

Analysis of the technical and administrative means of information protection illustrated by the example of the chosen logistics enterprise

Abstract

The information and informational technologies plays a very important role in the logistics activities and have a more and more greater influence on a market success of organization and keeping its competitiveness. Uninterrupted information flow makes basis for effective functioning of the supply chain. The information are exposed to various risks, which can lead to significant loss and damage. Therefore, the information security must be seen as an pivotal elements of the process logistics enterprise management.

In the article the identification of threats affecting on the level security information in the enterprise was presented. Also the analysis of the technical safety and administrative solution, which guarantee information security before threats. In the organization of this type of security lack creates incidents and events related to loss, modification and unauthorized access to data of the enterprise.

4. BIBLIOGRAFIA:

1. Ahuja V., *Bezpieczeństwo w sieciach*, Wyd. Mikom, Warszawa 1997.
2. Barczak A., Sydoruk T., *Bezpieczeństwo systemów informatycznych zarządzania*, Wyd. Bellona, Warszawa 2003
3. Białas A., *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, Wyd. Naukowo – Techniczne, Warszawa 2007.
4. Coyle J.J., Bardi E.J., Langrey Jr. J.C., *Zarządzanie logistyczne*, Wyd. PWE, Warszawa 2002.
5. Grabara J.K., Kisielnicki J., Nowak J.S., *Informatyka i współczesne zarządzanie*, Wyd. Polskie Towarzystwo Informatyczne, Katowice 2005.
6. Grabara J.K., Nowak J.S., *Systemy informatyczne – zastosowanie i wdrożenie cz.2*., Wyd. Naukowo Techniczne, Warszawa 2003.
7. Janczak J., Nowak A., *Bezpieczeństwo informacyjne. Wybrane problemy*, Wyd. AON, Warszawa 2012.
8. Kiełtyka L., *Komunikacja w zarządzaniu: techniki, narzędzia i formy przekazu informacji*, Wyd. Placet, Warszawa 2002.
9. Kifner T., *Polityka bezpieczeństwa i ochrony informacji*, Wyd. Helion, Gliwice 1999.
10. Norma PN-I-13335-1.
11. Nowe wyzwania, nowe rozwiązania, Polski Kongres Logistyczny, Logistics 2008.
12. Nowicki A., Sitarska M., *Procesy informacyjne w zarządzaniu*, Wyd. UE we Wrocławiu, Wrocław 2010.
13. Pańkowska M., *Zarządzanie zasobami informatycznymi*, Wyd. Difin, Warszawa 2001.
14. Prauzner T., *Prawo a bezprawie w Internecie*, [w:] Prace Naukowe Akademii im. Jana Długosza w Częstochowie, Tom IV, Wyd. AJD, red. A. Gil, Częstochowa 2009.
15. Prauzner T., *Technologia informacyjna – wybrane problemy społeczne*, [w] Edukacja-Technika-Informatyka nt: „*Wybrane problemy edukacji informatycznej i informacyjne*j", Rocznik Naukowy Nr 3/2012 cz.2, red. dr hab. prof. UR Walat W., Wyd. FOSZE, Rzeszów 2012.