STUDIA INFORMATICA 2001
Volume 22 Number 2 (44)

Andrzej BIAŁAS
SOTEL - Centrum Inżynierii Bezpieczeństwa Systemów Komputerowych i Telekomunikacyjnych

ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI W SYSTEMACH GOSPODARKI ELEKTRONICZNEJ

Streszczenie. Artykuł przedstawia przebieg procesu wdrażania zarządzania bezpieczeństwem informacji w przykładowej firmie e-biznesowej, począwszy od określenia celów i strategii bezpieczeństwa, stworzenia koncepcji zabezpieczeń, jej wdrożenia oraz działań mających na celu utrzymywanie osiągniętego poziomu bezpieczeństwa. Na tym tle przedstawiono typowe problemy bezpieczeństwa występujące w systemach gospodarki elektronicznej.

INFORMATION SECURITY MANAGEMENT IN e-COMMERCE SYSTEMS

Summary. Basing on fictitious company, assembling computers on demand sent by remote customers, paper presents all stages of implementation of an Information Security Management System. Starting from security objectives a system securing approach based on IT Security Baseline Protection Manual (BSI) is presented. Some security problems and baseline control in e-business were discussed.

1. Wstęp

Celem artykułu jest przedstawienie kompleksowego podejścia do problemu zabezpieczania złożonych systemów teleinformatycznych, na przykładzie zaczerpniętym z dziedziny gospodarki elektronicznej, oraz ukazanie na tym tle podstawowych problemów bezpieczeństwa spotykanych w tej dziedzinie. Artykuł stanowi zarazem przegląd zagadnień z obszaru zarządzania bezpieczeństwem informacji.

2. Bezpieczeństwo teleinformatyczne warunkiem rozwoju gospodarki elektronicznej

Wdrożenie technologii teleinformatycznych w instytucjach oraz powszechność zastosowań Internetu przynoszą ogromne korzyści, takie jak: przyspieszenie obrotu gospodarczego, zdobycie nowych rynków zbytu czy obniżenie kosztów działalności, ale ich skonsumowanie jest uwarunkowane zapewnieniem bezpieczeństwa informacji. Powierzenie systemom teleinformatycznym podstawowych zadań w instytucji oraz wszelkich zasobów informacji o znaczeniu strategicznym powoduje pełne uzależnienie się instytucji od niezawodnej i bezpiecznej pracy jej systemów.

W czasach dynamicznie rozwijającego się Internetu w społeczeństwie pojawiły się nowe relacje między gospodarką, sektorem finansowym, administracją a konsumentami. Wykorzystanie Internetu jako platformy do wymiany informacji między tymi sektorami stworzyło nowe możliwości rozwoju ekonomicznego i cywilizacyjnego społeczeństw - mówimy często o e-gospodarce, e-handlu, e-biznesie, a nawet o e-rządzie.

Niezwykle rozbudowane systemy teleinformatyczne gospodarki elektronicznej stawiają wysokie wymagania dotyczące bezpieczeństwa i niezawodności przetwarzania, przechowywania i przesyłania informacji, a Internet - jak wiadomo - nie był do takich celów projektowany. Mariaż nowych technologii, ich otwartość, rozproszenie oraz anonimowość użytkowników – wszystko to razem powoduje powstanie szeregu nieznanych dotąd form zagrożeń dla informacji – kluczowy stał się więc problem bezpieczeństwa tych nowych zastosowań teleinformatyki.

2.1. Kluczowe problemy bezpieczeństwa w systemach gospodarki elektronicznej

W systemach gospodarki elektronicznej można wyróżnić problemy bezpieczeństwa:

- typowe, podobne do problemów występujących w innych systemach teleinformatycznych,
- specyficzne, związane z szeroko pojętą ochroną elektronicznych transakcji handlowych.

Kluczowe problemy związane są z ochroną przed zagrożeniami podstawowych funkcji realizowanych przez gospodarkę elektroniczną.

2.1.1. Bezpieczeństwo wewnętrzne systemu

System teleinformatyczny realizujący funkcje użytkowe e-biznes podlega tym samym zagrożeniom, co inne systemy. Należy przewidzieć środki do ochrony elementów systemu, gdyż tylko wówczas osadzone w nim aplikacje mogą być bezpieczne. Tego typu problemy nie są czymś nowym. Należy się więc liczyć z koniecznością obrony przed:

- działaniem sił wyższych (katastrofy i klęski żywiołowe, rozruchy społeczne, itp.),
- przerwami w pracy sieci zasilającej,
- brakiem dostępności środków łączności, co ma istotny wpływ na bezpieczeństwo transakcji,
- zawirusowaniem systemu - zniszczeniem oprogramowania i danych,
- atakiem intruza wewnętrznego (nieuczciwego pracownika), który może dokonać nadużyć finansowych sam lub w ścisłej współpracy z którymś z klientów, np. może sfałszować transakcje,
- atakiem intruza zewnętrznego (hakera), który wykorzystując słabości systemu (np. łamiąc hasła) może zdobyć numery kart płatniczych lub sfałszować dane o płatnościach,
- nieumyślnymi i przypadkowymi, ale za to bardzo groźnymi w skutkach, pomyłkami użytkowników lokalnych lub zdalnych,
- wywołaniem przeciążenia systemu (atak typu Denial of Service), innymi przypadkami destabilizacji oraz destrukcji,
- upadkami systemu prowadzącymi do utraty bardzo ważnych informacji, np. dotyczących transakcji, kluczy szyfrujących, haseł itp.,
- pobraniem przez klienta niebezpiecznego oprogramowania z niepewnych źródeł (AciveX, aplety Java, konie trojańskie), które może np. przechwycić hasło klienta i dokonać w jego imieniu niekorzystnych transakcji.

Informacje dotyczące zamówień, dane osobowe, wiadomości pocztowe, dane uwierzytelniające, dane o płatnościach, czy o numerach kart płatniczych należą do niezwykle wrażliwych i stąd wymagają szczególnej ochrony.

Istnieje również niebezpieczeństwo manipulacji treścią ofert prezentowanych na witrynie, np. zmiana wartości cen, sfałszowanie opisu towaru lub nawet wystawienie ofert ośmieszających firmę lub działania cybergraffiti.

2.1.2. Bezpieczeństwo transakcji elektronicznych

Poważnym problemem są nieprawidłowo zakończone transakcje handlowe. Teoretycznie może się więc zdarzyć, że podczas operacji sprzedaży obciążanie konta bankowego klienta zakończy się poprawnie, zaś cała transakcja zakończy się z błędem - prowadzi to do obciążenia konta bez dostarczenia towaru do klienta.

Równie groźne w skutkach mogą być różnego typu zaprzeczenia: wysłania zamówienia przez klienta, przyjęcia zapłaty przez oferenta lub nawet wystawienia przez niego oferty.

2.1.3. Stworzenie platformy zaufania między partnerami biznesowymi

Zdarzają się dość często przypadki fałszowania tożsamości partnerów biorących udział w wymianie informacji biznesowych, np. podszywania się intruza, zwłaszcza pod atrakcyjną witrynę firmową. Niczego nie podejrzewający partnerzy firmy wymieniają z intruzem informacje jak z wiarygodną witryną i... np. mogą udostępnić intruzowi zbiór numerów kart płatniczych albo ulokować oszczędności na rzekomo lukratywnych warunkach.

3. Zarządzanie bezpieczeństwem informacji

Nie jest możliwe zapewnienie bezpieczeństwa współczesnych, niezwykle skomplikowanych systemów teleinformatycznych, zwłaszcza należących do sektora gospodarki elektronicznej, bez kompleksowego i interdyscyplinarnego podejścia do tego zagadnienia. Wymaga to współpracy specjalistów z wielu dziedzin, głównie: informatyków, prawników, ekspertów od zarządzania, a nawet fizyków. Poza tym bezpieczeństwo informacji, jako dyscyplina zawodowa, zmieniać się musi w tak szybkim tempie, jak szybko zmieniają się technologie informatyczne i ich zastosowania.

Doświadczenia i przemyślenia ekspertów od lat parających się tymi problemami, a także administratorów systemów, konstruktorów, programistów, zbierane są, porządkowane i publikowane w formie norm, wskazówek i zaleceń o zasięgu międzynarodowym lub krajowym [1-11]. Wzorując się na podstawowym dokumencie, jakim jest PN-I-13355 [6], spróbujemy przybliżyć trzy pojęcia, kluczowe dla dalszej części artykułu. Więcej szczegółów znaleźć można w [18],[24].

Bezpieczeństwo teleinformatyczne (ang. *IT security*) określa się jako wszelkie aspekty związane z definiowaniem, osiąganiem i utrzymywaniem tak zwanych atrybutów bezpieczeństwa, czyli: poufności, integralności, dostępności, rozliczalności, autentyczności i niezawodności.

Polityka bezpieczeństwa instytucji w zakresie systemów informatycznych (ang. *IT security policy*) obejmuje zasady, zarządzenia i procedury, które określają, jak zasoby – włącznie z informacjami wrażliwymi – są zarządzane, chronione i dystrybuowane w instytucji i jej systemach teleinformatycznych.

Zarządzanie bezpieczeństwem informacji (systemów informatycznych) (ang. *IT security management*) obejmuje zespół procesów zmierzających do osiągania, a potem utrzymywania ustalonego poziomu bezpieczeństwa, tzn. poziomu poufności, integralności, dostępności, rozliczalności, autentyczności i niezawodności. W zakres zarządzania bezpieczeństwem informacji wchodzą takie działania, jak:

- określenie celów (co należy chronić), strategii (w jaki sposób) i polityki bezpieczeństwa w instytucji (jakie konkretne przedsięwzięcia należy podjąć),
- identyfikowanie i analizowanie zagrożeń dla zasobów,
- identyfikowanie i analizowanie ryzyka,
- określenie adekwatnych zabezpieczeń,
- monitorowanie skuteczności wdrożonego systemu zabezpieczeń,
- opracowanie i wdrożenie programu szkoleniowo–uświadamiającego,
- wykrywanie i reakcja na incydenty.

Kluczowe procesy zarządzania bezpieczeństwem systemów teleinformatycznych to:

- proces zarządzania ryzykiem,
- proces zarządzania konfiguracją,
- proces zarządzania zmianami.

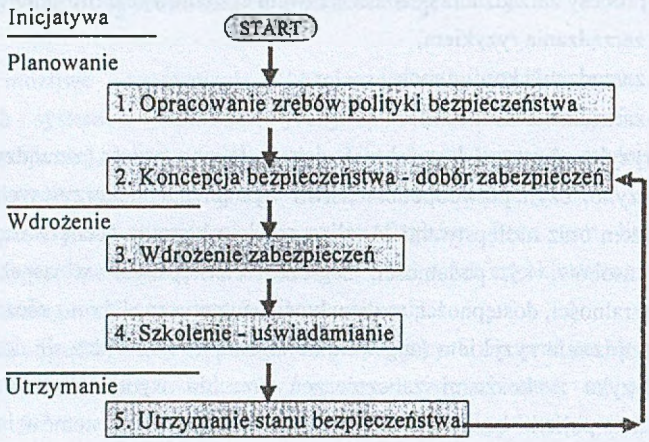
Analiza ryzyka (ang. *risk analysis*), jako główny proces zarządzania ryzykiem, identyfikuje ryzyko, czyli prawdopodobieństwo wystąpienia niekorzystnych zdarzeń wraz z ich scenariuszem oraz następstwami. Analiza ryzyka obejmuje ocenę wartości możliwych do stracenia zasobów, ich podatności, zagrożeń i następstw - w aspekcie naruszenia poufności, integralności, dostępności, rozliczalności, autentyczności oraz niezawodności.

Proces zarządzania ryzykiem (ang. *risk management*) sprowadza się do porównywania określonego ryzyka z kosztami zabezpieczeń oraz do wypracowywania strategii ich wdrożenia, a także polityki bezpieczeństwa instytucji w zakresie systemów informatycznych zgodnej z polityką bezpieczeństwa i celami działania instytucji. Po analizie kosztów potencjalnych następstw spośród wielu możliwych do zastosowania zabezpieczeń wybierane są właściwe. Jednocześnie zachodzi akceptacja ryzyka szczątkowego. Należy ponadto mieć na uwadze, że zabezpieczenia mogą wprowadzać własne podatności. Trzeba więc skupić uwagę nie tylko na redukcji znanego ryzyka, lecz również nie wprowadzać nowego, związanego z zabezpieczeniem.

Stosowane są różne metody analizy ryzyka. Niezależnie od tego jakiej użyjemy, decydująca jest równowaga między czasem i kosztem identyfikacji, kosztem zabezpieczeń a osiągniętym poziomem bezpieczeństwa. Analiza ryzyka jest dość pracochłonna, jednak nie zawsze musi być prowadzona. Często, zwłaszcza dla typowych systemów komercyjnych, wystarcza wprowadzenie tzw. **ochrony podstawowej** (ang. *baseline controls, baseline protection*), którą określa się jako minimalny zbiór typowych zabezpieczeń ustalony dla systemu lub instytucji. Jej przykładem jest metoda Ochrony Podstawowej Teleinformatyki, opracowana i udostępniona przez niemiecki Federalny Urząd Bezpieczeństwa Teleinformatycznego [11], opisana w [21],[22], a którą w dalszej części artykułu dla wygody będziemy oznaczać skrótem OPTI.

4. Wdrażanie zarządzania bezpieczeństwem informacji w systemach e-biznesowych

Proces wdrażania zarządzania bezpieczeństwem informacji, pokazany na rys. 1, jest wieloetapowy i musi zostać koniecznie zainicjowany przez świadome zagrożeń, ale i korzyści kierownictwo instytucji. Prezentowana tu procedura ogólna definiowania celów bezpieczeństwa, ich osiągania i utrzymywania, wynikająca z [1], [6], [11], przeniesiona została na grunt systemów gospodarki elektronicznej.



Rys. 1. Wdrożenie systemu zarządzania bezpieczeństwem informacji
Fig. 1. Implementation of Information Security Management System

4.1. Planowanie i koncepcja zabezpieczeń

Kierownictwo instytucji powołuje zespół odpowiedzialny za bezpieczeństwo informacji, wspierany często ekspertami z zewnątrz. Tworzona jest koncepcja zabezpieczeń oraz opracowane zostają zasady eksploatacji systemów w instytucji. Sprowadza się to do wykonania szeregu analiz zasobów, zagrożeń i podatności, wytyczenia celów, strategii i polityki bezpieczeństwa, a w końcu do zaprojektowania zabezpieczeń adekwatnych do wielkości zagrożeń, wartości zasobów oraz potencjalnych następstw.

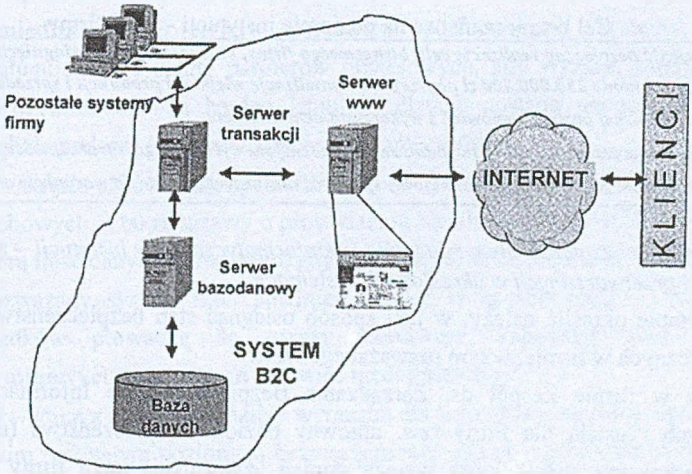
4.1.1. Określenie celów, strategii i polityki bezpieczeństwa

Rozważmy fikcyjną firmę *ABC*, zajmującą się produkcją komputerów według indywidualnych specyfikacji, napływających od klientów za pośrednictwem Internetu.

Wdrożenie systemu B2C (Business to Customer) pozwala szybko reagować na zróżnicowane potrzeby klientów, a przez co uzyskiwać przewagę nad konkurencją.

Rys. 2 przedstawia zasadnicze elementy typowego systemu B2C, realizującego obsługę strumienia zamówień. W rzeczywistości musi on być bardziej rozbudowany, a ponadto powinien współpracować z innymi wydzielonymi systemami teleinformatycznymi tej firmy, z których każdy wpływa w określony sposób na realizację misji firmy ABC. Jej celem biznesowym jest uzyskiwanie jak najwyższych dochodów z produkcji i sprzedaży komputerów. Podstawowymi elementami rozważanego systemu obsługi transakcji są:

- **serwer www** - za pomocą atrakcyjnej zaprojektowanej witryny prezentuje katalog możliwych wariantów konstrukcyjnych wyrobów oraz ich możliwości, służy klientom do dokonywania transakcji handlowych i śledzenia stanu ich realizacji za pomocą Internetu, dynamicznie odzwierciedla stan baz danych (zapasów),
- **serwer transakcji**, działa w tle witryny i obsługuje bieżące transakcje: zapytania o możliwość realizacji zamówień, same zamówienia, płatności, rozliczenia itp.,
- **serwer bazodanowy** zarządza odwołaniami do baz danych i uzyskiwanymi w ich wyniku odpowiedziami - wykonanie każdej transakcji implikuje bowiem szereg operacji na bazach danych: kwerendy, modyfikacje rekordów, usuwanie rekordów itp.



Rys. 2. Przykładowy system handlu elektronicznego
Fig. 2. Example of typical e-commerce system

Powszechnie stosuje się [6] trójpoziomowy model bezpieczeństwa, który wyróżnia:

- bezpieczeństwo w instytucji (jej misji),
- bezpieczeństwo systemów teleinformatycznych w instytucji,
- bezpieczeństwo konkretnego systemu teleinformatycznego.

Dla całej instytucji oraz dla każdego z tych poziomów można określić:

- cele bezpieczeństwa – co chcemy osiągnąć?
- strategię – w jaki sposób osiągnąć te cele?
- politykę (działania) – co konkretnie należy zaplanować i wykonać?

Ponadto, cele bezpieczeństwa instytucji wpływają na strategie bezpieczeństwa teleinformatycznego w instytucji, te zaś są rozwijane w postaci planów zabezpieczeń poszczególnych systemów, realizujących polityki. Hierarchię tę wykorzystuje się w procesie transformacji celów, poprzez strategie, do planów szczegółowych. Ta konkretyzacja prowadzi w końcu do wyznaczenia listy zabezpieczeń, co dalej zostanie pokazane.

Określenie globalnego celu bezpieczeństwa

Celem biznesowym (misją) jest maksymalizacja zysków ze sprzedaży, zaś celem bezpieczeństwa na poziomie instytucji jest zapewnienie bezpieczeństwa realizacji celu biznesowego. Misja tej przykładowej firmy, przedstawiona w tabeli 1, realizowana jest przez trzy strategie, z których pierwsza jest silnie zależna od sprawnej i bezpiecznej obsługi elektronicznych transakcji handlowych.

Tabela 1

Cel bezpieczeństwa na poziomie instytucji - misji firmy

Należy zapewnić bezpieczną realizację celu biznesowego firmy, polegającego na osiągnięciu dochodów ze sprzedaży na poziomie 250.000.000 zł poprzez maksymalizację wielkości produkcji i sprzedaży, dzięki:
• *zapewnieniu sprawnej obsługi zamówień z wykorzystaniem Internetu,*
• *zapewnieniu wystarczających zasobów finansowych, potencjału wytwórczego, atrakcyjności produktów,*
• *utrzymywaniu dobrego wizerunku i opinii firmy sprawnie dostosowującej się do warunków otoczenia.*

Cele i strategie bezpieczeństwa systemów teleinformatycznych w instytucji – grup informacji przetwarzanych w określonych systemach

Na tym etapie określić należy, w jaki sposób osiągnąć stan bezpieczeństwa systemów teleinformatycznych w firmie, w tym rozważanego B2C.

Powołany w firmie Zespół ds. Zarządzania Bezpieczeństwem Informacji dokonuje analizy potrzeb i ustala dla firmy tzw. umowny poziom bezpieczeństwa (maksymalny, wysoki, umiarkowany, niski), który wyraża stopień uzależnienia misji firmy od środków teleinformatycznych i ich bezpieczeństwa, a w konsekwencji zadecyduje o późniejszym doborze zabezpieczeń. Rozważenie kilku poniższych kwestii dla przykładowego B2C pomoże w wyznaczeniu tego poziomu:

- **Informacjami poufnymi**, wymagającymi **szczególnej ochrony**, są dane dotyczące transakcji, zwłaszcza informacje finansowe, dane osobowe oraz dane, których ujawnienie naraziłoby na straty kontrahentów oraz osoby zainteresowane. **Poufność informacji** wymagana jest więc na **użytek wewnętrzny** oraz **dla ochrony interesów partnerów biznesowych.**
- **Dokładność i dostępność** informacji dotyczących strumienia i stanu realizacji zamówień, informacji przekazywanych do innych systemów działających w firmie, informacji finansowych **wpływają znacząco na bieżące decyzje** podejmowane przez kierownictwo firmy.
- **Ważnym zadaniem** firmy, możliwym do realizacji **tylko za pomocą środków teleinformatycznych,** jest właśnie zadanie realizowane przez system B2C, czyli przyjmowanie i realizacja zamówień poprzez Internet.
- Niewątpliwie do **zadań złożonych,** możliwych do realizacji **tylko przez środki teleinformatyczne,** należą transakcje handlowe oraz wynikające z nich operacje bazodanowe.
- Szczególnie **atrakcyjnymi dla intruzów celami** mogą być informacje handlowe umożliwiające dokonanie nadużyć finansowych oraz informacje cenne dla konkurencji. Firma *ABC* cieszy się dobrą reputacją i w związku z tym sfałszowanie informacji lub cybergraffiti na jej witrynie może być przedmiotem dumy i uznania w środowisku hakerskim.
- **Zaniedbania ze strony personelu** obsługującego systemy, personelu obsługującego systemy partnerów biznesowych, **siły wyższe, błędy sprzętowe i programowe** – są bardzo istotne i dlatego zostaną poddane szczegółowej analizie podczas tworzenia koncepcji bezpieczeństwa.
- W zakresie **aktów prawnych** istotne są postanowienia ustawy o ochronie danych osobowych, a także ustawy o prowadzeniu handlu na odległość. Firma przetwarza sporą ilość danych osobowych, gdyż wielu jej klientów to osoby fizyczne.
- Rozważany system B2C powinien działać w sposób ciągły. Dłuższe okresy upadków prowadzą do **utraty zamówień, reputacji oraz naruszenia terminowych zobowiązań** - są więc niedopuszczalne.

Jak często wynika z dogłębnej analizy wymagań dla tego typu systemów, ogólnie cechują się one wysokim umownym poziomem bezpieczeństwa, jednak w pewnych obszarach może się on okazać umiarkowany.

Wyznaczając umowny poziom bezpieczeństwa, wspomniany Zespół opracował właściwie pierwszą część dokumentu polityki bezpieczeństwa - rozdział p. t. ***„Znaczenie bezpieczeństwa teleinformatycznego dla misji firmy ABC"***. Należy zauważyć, że ten dokument dotyczy całej firmy, jednak rozważania ograniczono tu do podsystemu B2C.

Wspomniany rozdział określa zespół celów i strategii bezpieczeństwa - ogólnych dla systemów teleinformatycznych oraz specyficznych dla przykładowego systemu gospodarki elektronicznej (tabela 2). Dokument ten będzie uzupełniany i aktualizowany podczas całego procesu wdrażania zarządzania bezpieczeństwem informacji w instytucji, bowiem cele i strategie są podstawą projektu zabezpieczeń, ich wdrożenia, opracowania zasad eksploatacji systemów w instytucji, działań szkoleniowo-uświadamiających, zasad monitorowania osiągniętego stanu bezpieczeństwa, reagowania na incydenty itp. - wszystkie te działania muszą być zwięźle określone w dokumencie polityki bezpieczeństwa unikalnym w tym sensie, że możliwym do wykorzystania tylko w firmie ABC dopóty, dopóki jej systemy teleinformatyczne będą służyć realizacji misji tej firmy.

Dla systemów gospodarki elektronicznej można sformułować zwykle trzy cele bezpieczeństwa [23],[14], przedstawione w tabeli 2. Każdy jest realizowany przez określoną grupę strategii, a te będą podstawą projektu zabezpieczeń.

Tabela 2

Cele i strategie bezpieczeństwa przykładowego systemu B2C

Cel 1: Należy zapewnić bezpieczeństwo wewnętrzne systemu (sprzętu, oprogramowania systemowego, aplikacji oraz środków komunikacji), stanowiące podstawę realizacji osadzonych w nim funkcji e-biznesowych, poprzez:
(strategia związana z celem 1): • *zapewnienie wysokiego poziomu niezawodności, ciągłej dostępności usług oferowanych przez serwery, z możliwością tolerowania jedynie krótkotrwałych upadków,* • *stały nadzór wszelkich (dopuszczalnych i niedopuszczalnych) aspektów aktywności serwerów - skrupulatna rozliczalność,* • *wykluczenie możliwości dokonywania nadużyć na serwerach przez intruzów wewnętrznych lub zewnętrznych,* • *zapewnienie poufności, integralności i dostępności przetwarzanych danych,* • *ochronę środków zainwestowanych w sprzęt, oprogramowanie systemowe i aplikacje, środki teletransmisji, informacje biznesowe, procesy wytwarzania oraz wiedzę zgromadzoną w firmie,* • *zapewnienie możliwości odzyskiwania utraconych informacji,* • *priorytetowe traktowanie jakości informacji, co ma wpływ na efektywność obsługi strumienia zamówień oraz decyzje podejmowane przez zarząd, w tym dotyczące wszystkich procesów w firmie,* • *respektowanie wymagań narzuconych przez ustawy (ochrony danych osobowych, prowadzenie handlu na odległość),* • *przedsięwzięcie środków ofensywnych (zabezpieczenia techniczne, organizacyjne, personalne) zmierzających do unikania incydentów i ochrony przed ich skutkami,* • *wyczulenie personelu obsługi na bezpośrednie zagrożenie dotyczące ciągłości misji firmy.*
Cel 2: Należy zapewnić bezpieczeństwo przetwarzanych, przechowywanych, a zwłaszcza przesyłanych informacji, poprzez:
(strategia związana z celem 2): • *uniemożliwienie manipulacji na danych przesyłanych, zwłaszcza związanych z zamówieniami,*

płatnościami, dostawami, oraz wycofywanie transakcji podejrzanych o manipulację,

- *zapewnienie poufności przesyłanych informacji, w szczególności danych osobowych, danych o przepływie płatności,*
- *zapewnienie terminowości realizacji transakcji elektronicznych z partnerami,*
- *uniemożliwienie powtórnego wykorzystanie danych związanych z transakcjami,*
- *zapewnienie niezaprzeczalności dokonania zapłaty, zamówienia lub dostawy,*
- *stałe utrzymywanie atrakcyjności i wydajności obsługi witryny, przyczyniając się do utrzymywania pozytywnego wizerunku firmy,*
- *zachowanie szczególnej czujności wobec cybergraffiti oraz przeciążeń.*

Cel 3: Należy zapewnić kontrolę autentyczności podmiotów prowadzących e-biznes, poprzez:

(strategia związana z celem 3):

- *stosowanie zaawansowanych technologii uwierzytelnień,*
- *wymianę podpisanych dokumentów potwierdzających operacje.*

Reasumując, dokument polityki bezpieczeństwa w fazie początkowej może mieć postać ramową, przedstawioną na rys. 3.

Polityka bezpieczeństwa firmy ABC

w pierwszej fazie określana jest ogólnie polityka oraz zasoby ludzkie

1. Znaczenie bezpieczeństwa teleinformatyki (TI) dla realizacji misji firmy
   Znaczenie TI dla realizacji zadań naszej instytucji
   Zakładany (umowny) poziom bezpieczeństwa
   Cele bezpieczeństwa związane ze stosowaniem TI w firmie
2. Raport o powołaniu Zespołu ds. Zarządzania Bezpieczeństwem TI
   decyzja pisemna ze wskazaniem kompetencji
3. Wyznaczenie inspektora ds. Bezpieczeństwa TI (IT Security Officer)
   decyzja pisemna ze wskazaniem kompetencji
4. Określenie zasad odpowiedzialności personelu w zakresie bezpiecznej eksploatacji środków informatycznych
   decyzja pisemna ze wskazaniem kompetencji

w miarę realizacji kolejnych zadań uzupełniamy o:

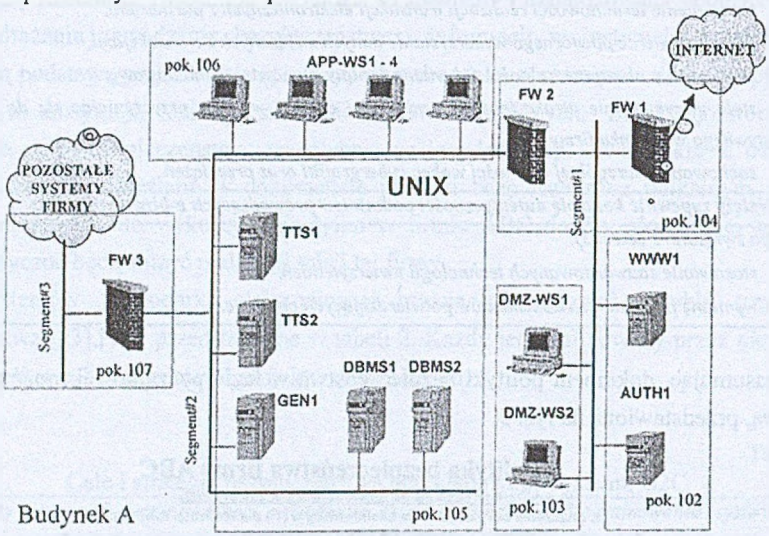
5. Plan implementacji (wdrożenia) zabezpieczeń
6. Plan szkoleń i działań pogłębiających świadomość bezpiecznego wykorzystania środków teleinformatycznych
7. Utrzymywanie osiągniętego poziomu bezpieczeństwa - kontrole, rewizje, reakcje na naruszenia

Rys. 3. Zawartość dokumentu polityki bezpieczeństwa
Fig. 3. Contents of IT Security Policy

4.1.2. Identyfikacja elementów systemów teleinformatycznych

Z wyznaczonych celów bezpieczeństwa wynika, że skrajnie uproszczony schemat funkcjonalny systemu B2C (rys. 2) musi zostać uzupełniony o typowe zabezpieczenia, takie jak: systemy zaporowe, serwery uwierzytelnień, narzędzia do tworzenia prywatnych sieci wirtualnych (VPN), stanowiska nadzoru, które tam pominięto, a bez których nie można zrealizować postawionych celów. Wynika stąd, że pewnego typu zabezpieczenia samoistne, wynikające bezpośrednio z określonych powyżej celów i strategii, muszą być wprowadzone na samym wstępie, natomiast szczegóły ich architektury, konfiguracji są określane podczas

doboru innych zabezpieczeń. Nawet tak rozbudowany system, który pokazano na rys. 4, jest nadal bardzo uproszczony w stosunku do systemów rzeczywistych i będzie służył tu tylko do zilustrowania procedury doboru zabezpieczeń OPTI.



Rys. 4. Schemat blokowy rozważanego systemu B2C
Fig. 4. Considered B2C system's scheme

Przykładowy system, zbudowany w oparciu o technologię UNIX®, zawiera segmenty sieci Ethernet®, dzielące wraz z zaporami system na trzy części:

- strefa zdemilitaryzowana (segment#1), w której pracują dwa stanowiska nadzoru sieci, serwer WWW1 oraz serwer uwierzytelniający AUTH1, służący użytkownikom wewnętrznym, mobilnym oraz zdalnym partnerom biznesowym,
- strefa aplikacji e-biznesowych (segment#2), w której odbywa się przetwarzanie transakcji handlowych w serwerach TTS1, TTS2, współpracujących z systemami zarządzania bazami danych DBMS1, DBMS2; działają tu również serwer ogólnego przeznaczenia GEN1 oraz kilka stanowisk obsługi,
- inne systemy firmy (segment#3 i dalsze) - finanse, wspomaganie kierownictwa, ERP itp. zostały wyraźnie odizolowane od rozważanego.

Z wykorzystaniem wzorcowych formularzy spisowych OPTI zbierane są informacje o elementach systemów teleinformatycznych (tabela 3, rys. 4). Uwzględnia się ich umiejscowienie oraz użytkowników. Rozróżnia się typy:

- stanowiska samodzielne lub klienckie,
- sieć działająca w oparciu o serwer,
- środki transmisji danych (telekomunikacji).

Tabela 3

Istniejące i planowane elementy systemu B2C

Lp.	Nazwa i opis	Gdzie się znajduje	Typ	Połączenia sieciowe, usługi	Status	Użytkownicy
1	Serwer www „WWW1" /UNIX System	Budynek A Serwerownia pok.102	Serwer	Ethernet Segment #1 FTP, e-mail, funkcje B2C	działający	Pracownicy Komórki B2C-DMZ
2	Serwer uwierzytelniający „AUTH1" /UNIX System	Budynek A Serwerownia pok.102	Serwer	Ethernet Segment #1 Uwierzytelnianie	testowany	Pracownicy Komórki B2C-DMZ
3	Stanowisko nadzoru „DMZ-WS1" /UNIX System	Budynek A Biuro pok.103	Klient	Ethernet Segment #1 Drukarka laserowa	działający	Pracownicy Komórki B2C-DMZ
4	Stanowisko nadzoru „DMZ-WS2" /UNIX System	Budynek A Biuro pok.103	Klient	Ethernet Segment #1	działający	Pracownicy Komórki B2C-DMZ
5	Zapora ograniczająca FW1"	Budynek A Pom. techniczne pok.104	Transmisja danych	Ethernet Segment #1 Router	działający	Pracownicy Komórki B2C-DMZ
6	Zapora ograniczająca „FW2"	Budynek A Pom. techniczne pok.104	Transmisja danych	Ethernet Segment #1 Ethernet Segment #2	działający	Pracownicy Komórki B2C-DMZ
7	Serwer transakcji „TTS1" /UNIX System	Budynek A Serwerownia pok.105	Serwer	Ethernet Segment #2	testowany	Pracownicy Działu B2C-APP
8	Serwer transakcji „TTS2" /UNIX System	Budynek A Serwerownia pok.105	Serwer	Ethernet Segment #2	testowany	Pracownicy Działu B2C-APP
9	Serwer bazodanowy „DBMS1" /UNIX System	Budynek A Serwerownia pok.105	Serwer	Ethernet Segment #2	działający	Pracownicy Działu B2C-APP
10	Serwer bazodanowy „DBMS1" /UNIX System	Budynek A Serwerownia pok.105	Serwer	Ethernet Segment #2	działający	Pracownicy Działu B2C-APP
11	Serwer sieciowy „GEN1" /UNIX System	Budynek A Serwerownia pok.105	Serwer	Ethernet Segment #2	działający	Pracownicy Działu B2C-APP
12	Stanowisko nadzoru „APP-WS1" /UNIX System	Budynek A Biuro pok.106	Klient	Ethernet Segment #2	działający	Pracownicy Komórki B2C-APP
13	Stanowisko nadzoru „APP-WS2" /UNIX System	Budynek A Biuro pok.106	Klient	Ethernet Segment #2	działający	Pracownicy Komórki B2C-APP
14	Stanowisko nadzoru „APP-WS3" /UNIX System	Budynek A Biuro pok.106	Klient	Ethernet Segment #2,	planowane	Pracownicy Komórki B2C-APP
15	Stanowisko nadzoru „APP-WS4" /UNIX System	Budynek A Biuro pok.106	Klient	Ethernet Segment #2, Drukarka laserowa	działający	Pracownicy Komórki B2C-APP
13	Zapora ograniczająca „FW3"	Budynek A Pom. techniczne Pok. 107	Transmisja danych	Ethernet Segment #2 Ethernet Segment #3	działający	Pracownicy Komórki B2C-MAN

Składniki systemu B2C z tabeli 3 wybrano dla potrzeb ilustracji metody OPTI, nie zaś z punktu widzenia efektywności systemu B2C – meritum problemów projektowania systemów gospodarki elektronicznej nie jest przedmiotem zainteresowań tego artykułu. Można więc przyjąć, że mamy tu do czynienia z systemem Unix® (sieć, serwery i klienci), odizolowanym systemami zapór.

4.1.3. Identyfikacja aplikacji oraz przetwarzanych przez nie informacji

Załóżmy, że rozważany system B2C podzielić można na kilka mniejszych, ściśle ze sobą współpracujących aplikacji, co pokazano w tab.4. Każda z nich przetwarza określoną grupę informacji i jest związana także z pewnymi aktywami nie będącymi informacjami, np. serwer WWW decyduje o wizerunku firmy, serwer przetwarzający transakcje decyduje o zdolności do świadczenia usług itp.

Tabela 4

Istniejące i planowane aplikacje

Lp.	Nazwa i opis	Lista aplikacji pracujących na zidentyfikowanych elementach systemu B2C	Informacje i inne aktywa z nimi związane
1	Serwer www „WWW1" /UNIX System	Dynamiczna prezentacja oferty firmowej Interaktywna obsługa partnerów biznesowych	Oferta firmowa, formularze, wiadomości pocztowe związane z obsługą witryny, wizerunek firmy
2	Serwer uwierzytelniający „AUTH1" /UNIX System	Serwer kluczy publicznych Oprogramowanie uwierzytelniające	Dane uwierzytelniające, klucze szyfrujące
3	Stanowiska nadzoru „DMZ-WS1 - 2" /UNIX System	Oprogramowanie klienckie	Raporty dotyczące działania serwerów
4	Serwer transakcji „TTS1 - 2" /UNIX System	Obsługa transakcji handlowych	Dane związane z transakcjami handlowymi Dane osobowe Zdolność do świadczenia usług
5	Serwer bazodanowy „DBMS1 - 2" /UNIX System	Aplikacja bazodanowa B2C	Baza danych o operacjach handlowych Dane osobowe
6	Serwer sieciowy „GEN1" /UNIX System	Serwer plików Serwer dokumentów	Raporty zbiorcze o przeprowadzonych transakcjach dla kierownictwa
7	Stanowisko nadzoru „APP-WS1 do 4" /UNIX System 0	Konsola operatora nadzoru sieci	Raporty, dzienniki

4.1.4. Określenie wymagań ochronnych dla elementów systemu

Wymagania ochronne ustala się na podstawie oceny następstw w sześciu kategoriach, [11], [22] w toku dość pracochłonnej analizy, pomijanej tu ze względu obszerność zagadnienia. Prowadzi ją Zespół ds. Zarządzania Bezpieczeństwem Informacji, przy znaczącym udziale użytkowników. Odbywa się to dla każdego zidentyfikowanego elementu systemu, na którym działają określone aplikacje, z którymi związane są pewne informacje, charakteryzowane przez atrybuty poufności, integralności i dostępności. Każdy w ten sposób określony element systemu zostaje poddany analizie zagrożeń i następstw w myśl zasady *„Co się stanie, jeśli...?"*.

W toku analizy należy stosować metodę najgorszego przypadku, uwzględniać wzajemne zależności między elementami systemów oraz efekt kumulacji następstw. Załóżmy, że po przeprowadzeniu analizy otrzymano następujące wartości wymagań ochronnych, pokazane w tabeli 5. Wynika z niej jasno, jaki jest możliwy zakres wykorzystania metody ochrony

podstawowej (wymagania „niskie do umiarkowanych"), a dla jakich elementów systemu należy się posiłkować analizą ryzyka (wymagania „wysokie", „bardzo wysokie").

Tabela 5

Przykład określenia wymagań ochronnych dla elementów systemu

Nazwa przykładowego składnika systemu	Wartość chroniona	Wymaganie ochronne	Uzasadnienie
Serwer www	poufność	umiarkowane	Serwer tylko pośredniczy w wymianie informacji
„WWW1"	integralność	umiarkowane	Istnieje możliwość odtworzenia witryny
	dostępność	wysokie	Partnerzy dopuszczają możliwość wyłączenia do 1,5 godziny
Serwer uwierzytelniający	poufność	bardzo wysokie	Poufność danych uwierzytelniających jest podstawą bezpieczeństwa całego systemu
„AUTH1"	integralność	wysokie	Integralność danych uwierzytelniających jest podstawą bezpieczeństwa całego systemu
	dostępność	wysokie	Partnerzy dopuszczają możliwość wyłączenia do 1,5 godziny
Stanowiska nadzoru	poufność	umiarkowane	Mogą tu być informacje do wykorzystania jedynie przez bardzo doświadczonych intruzów
„DMZ-WS1 - 2"	integralność	wysokie	Informacje decydują o możliwości skutecznej obrony przed atakiem
(rozważane wspólnie)	dostępność	wysokie	Informacje decydują o możliwości skutecznej obrony przed atakiem
Serwer transakcji	poufność	wysokie	Ujawnienie powoduje duże szkody
„TTS1 - 2"	integralność	bardzo wysokie	Manipulacja informacjami związanymi z transakcjami może przynieść znaczne szkody dla firmy i jej partnerów
(rozważane wspólnie)	dostępność	wysokie	Niedostępność serwera transakcji paraliżuje działalność handlową firmy - 1,5 godzinne wyłączenia są dopuszczalne
Serwer bazodanowy	poufność	wysokie	Ujawnienie powoduje duże szkody (informacje finansowe i dane osobowe)
„DBMS1 - 2"	integralność	umiarkowane	Baza może być szybko naprawiona
(rozważane wspólnie)	dostępność	wysokie	1,5 -godzinne wyłączenia są dopuszczalne
Serwer sieciowy	poufność	wysokie	Poufność raportów kierowanych do kierownictwa jest konieczna
„GEN1"	integralność	wysokie	Raporty dla kierownictwa o prowadzonych transakcjach - informacje o własnym statusie wpływają znacząco na decyzje kierownictwa.
	dostępność	niskie	Raporty można przesyłać raz na dobę
Stanowiska nadzoru	poufność	umiarkowane	Ujawnienie tych informacji jest dość groźne
„APP-WS1 do 4"	integralność	wysokie	Utrata zdolności do oceny rezultatów gospodarczych - zafałszowanie własnej „tożsamości"
(rozważane wspólnie)	dostępność	umiarkowane	Raporty można przesyłać raz na dobę

Przyjęte w przykładzie wartości wymagań są dość umowne. Funkcje e-biznesowe skupiono w bardzo okrojonym systemie, w którym wszystkie elementy w istotny sposób wpływają na bezpieczeństwo, stąd otrzymano relatywnie wysokie wymagania ochronne,

które właściwie uniemożliwiają wprost zastosowanie OPTI bez wsparcia przez analizę ryzyka. W rzeczywistych systemach funkcjonalność jest bardziej rozproszona, stosuje się redundancje elementów, poza tym nie wszystkie systemy e-biznes mają tak wysokie wymagania, jak pokazano na przykładzie.

Użyteczność OPTI polega na tym, że najpierw można zapewnić ochronę podstawową systemu, by później przeprowadzić analizę ryzyka i udoskonalić pewne zabezpieczenia.

4.1.5. Modelowanie systemu i dobór zabezpieczeń

Z tabeli 3 wynika, że rozważany system B2C firmy *ABC* jest siecią wykorzystującą serwery, zbudowaną w oparciu o system Unix® oraz Ethernet®, wyposażoną w trzy zapory ograniczające. System został umiejscowiony w kilku pomieszczeniach budynku A firmy i jest obsługiwany przez dwie grupy operatorów B2C-APP, B2C-DMZ. Grupę B2C-MAN i inne nie wyszczególnione pomijamy, gdyż działają one na zewnątrz rozważanego systemu. Przyjęto też inne założenia upraszczające: w firmie ABC brak jest komputerów przenośnych (notebooków), samodzielnych stanowisk roboczych, są tylko stacje klienckie - wyłącznie uniksowe, brak jest faksów, automatycznych sekretarek, pominięto urządzenia telekomunikacyjne itp.

Modelowanie systemu B2C polega na przypisaniu rzeczywistym systemom komponentów z katalogu. Mamy tu do czynienia **z jednym** rzeczywistym systemem - **siecią wyposażoną w serwery** działającą w środowisku Unix®. Zgodnie z [11] jej funkcjonalność zostaje wyrażona za pomocą wybranych komponentów, przedstawionych w tabeli 6. Korzystne jest, aby samo modelowanie przeprowadzić w pięciu etapach, łącząc pewne zagadnienia w grupy.

Etap 1: Ogólne aspekty bezpieczeństwa

Koncepcja tworzenia kopii zapasowych dla każdego serwera może być różna, więc komponent 3.4 należy wstawić tyle razy, ile różnych koncepcji wystąpi. Prawdopodobnie będzie to sześć komponentów po jednym dla każdego typu serwera oraz 1 komponent dla wszystkich stacji roboczych. Pozostałe komponenty wystąpią jednokrotnie.

START

Tabela 6

Modelowanie przykładowego systemu B2C

Nr	Nazwa grupy lub komponentu	Etap 1 Aspekty ogólne	Etap 2 Infrastruktura	Etap 3 Stanowiska	Etap 4 Sieci	Etap 5 Aplikacje
	OCHRONA KOMPONENTÓW					
3.1	Organizacja	1				
3.2	Personel	2				
3.3	Zdarzenia przypadkowe	3				
3.4	Kopie zapasowe	4				
3.5	Ochrona prywatności danych	5				
3.6	Ochrona antywirusowa	6				
3.7	Ochrona kryptograficzna	7				
3.8	Sytuacje nadzwyczajne	8				
	INFRASTRUKTURA					
4.1	Budynki		9			
4.2	Okablowanie		10			
4.3.1	Pomieszczenia biurowe		11			
4.3.2	Serwerownia		12			
4.3.3	Magazyn nośników		13			
4.3.4	Pomieszczenia dla infrastruktury technicznej		14			
4.4	Szafy ochronne		15			
4.5	Praca na komputerze domowym					
	SYSTEMY NIE PODŁĄCZONE DO SIECI					
5.1	Komputer z systemem DOS (jeden użytkownik)					
5.2	Komputer z systemem Unix			16		
5.3	Komputer przenośny (notebook)					
5.4	Komputer z DOS (wieloużytkownikowy)					
5.5	Komputer z Windows NT					
5.6	Komputer z systemem Windows 95					
5.99	Samodzielne stanowisko (Stand-alone IT system)					
	SYSTEMY SIECIOWE					
6.1	Sieci wyposażone w serwery				17	
6.2	Sieci z Unix				18	
6.3	Sieci typu Peer-to-Peer					
6.4	Sieci z Windows NT					
6.5	Novell Netware 3.x					
6.6	Novell Netware 4.x					
6.7	Sieci heterogeniczne				19	
6.8	Zarządzanie sieciami i systemami				20	
	SYSTEMY PRZESYŁANIA DANYCH					
7.1	Wymiana danych na nośnikach					
7.2	Modemy					
7.3	System zaporowy				21	
7.4	Poczta elektroniczna				22	
7.5	Serwer WWW				23	
	TELEKOMUNIKACJA					
8.1	Systemy telekomunikacyjne (PBX, ISDN)					
8.2	Faks					
8.3	Sekretarka automatyczna					

Dla każdego serwera i typu stanowiska oddzielnie

Oddzielnie dla okablowania elektrycznego i transmitującego dane

Dla każdej z 3 zapór oddzielnie

8.4	Połączenia sieci lokalnych przez ISDN					
	INNE SKŁADNIKI SYSTEMU					
9.1	Oprogramowanie standardowe					24
9.2	Bazy danych					25
9.3	Telekomutacja					

KONIEC

Etap 2: Infrastruktura

Wyklucza się komponent 4.5 (praca w domu). Ze względu że cały system mieści w jednym budynku, to 4.1 wystąpi raz. Komponent 4.2 zostanie użyty dwukrotnie - oddzielnie dla okablowania elektrycznego i dla transmitującego dane. Zakładając, że obie serwerownie są identyczne (pok. 102, 105), podobnie biura (pok. 103, 106) przeznaczone na stanowiska robocze oraz pomieszczenia techniczne z urządzeniami transmisji oraz zaporami (pok. 104, 107), to wystarczy wstawić po jednym komponencie 4.3.2, 4.3.1 oraz 4.3.4. Przewidziano dwie identyczne szafy ochronne na nośniki zapasowe po jednej dla każdego biura, stąd komponent 4.4 wystąpi jednokrotnie. Komponent 4.3.3 - dodatkowe pomieszczenie na archiwizowane nośniki musi zostać dopiero wydzielone i odpowiednio przystosowane.

Etap 3: Stanowiska samodzielne i klienckie

Wszystkich 6 stanowisk jest identycznych - komponent 5.2 wstawiony zostaje jednokrotnie.

Etap 4: Bezpieczeństwo sieciowe

Sieć z systemem UNIX® wyposażoną w serwery modelują komponenty 6.1 oraz 6.2. Należy też wstawić 6.7, gdyż sieci zawierają różnego typu przełączniki pasywne i aktywne. Sieć jest zarządzana, więc pojawia się 6.8. Zastosowane zapory ograniczające różnią się przeznaczeniem (architekturą), więc komponent 7.3 pojawi się trzykrotnie.

Etap 5: Aplikacje

Przyjmując, że w systemie działa jedna wielostanowiskowa bazodanowa aplikacja B2C, to ten fakt można zamodelować parą komponentów 9.1, 9.2.

Etap 6: Kontrola zupełności modelu systemu

Po zamodelowaniu systemu należy sprawdzić, czy model całego systemu jest kompletny.

Tablica 6 wyznacza pewną marszrutę uzyskaną podczas modelowania (kroki od 1 do 25), którą należy przejść, przy czym krok nr 4 będzie wykonany sześciokrotnie (5 typów serwerów, 1 typ stanowisk klienckich), krok nr 10 dwukrotnie, a krok nr 21 trzykrotnie, gdyż założono, że zapory różnią się architekturą.

Nawet dla tak skrajnie uproszczonego systemu należy więc przeanalizować 33 komponenty standardowych zabezpieczeń OPTI, a każdy z komponentów to wyodrębnione

zagadnienie bezpieczeństwa. Rozważania muszą zostać ograniczone do pewnego przykładu, dotyczącego serwera www.

Ogólny tok postępowania przebiega w następujący sposób. Należy więc dla każdego z 25 kroków:

- przeanalizować przyporządkowany mu komponent - czasem wielokrotnie - w kontekście specyfiki modelowanego obiektu, np. tu zapoznać się z rozdziałem pt. **7.5 Serwer WWW** [11],
- przejrzeć wszystkie wyspecyfikowane dla niego zagrożenia, przykładowo tabela 7 przedstawia ich wykaz, które należy przeanalizować dla rozważanego systemu - analiza zagrożeń jest pomocna, choć w OPTI opcjonalna; tabela zawiera listę odnośników do katalogu zagrożeń, np. w rozdziale T2.2 można zapoznać się z problemem *„Niewystarczająca wiedza na temat procedur bezpieczeństwa"*,
- przejrzeć zabezpieczenia zalecane przez ochronę podstawową i porównać je z istniejącymi. Dokonuje się tego za pomocą formularza - ankiety przygotowanej dla każdego z komponentów (dostępne w wersji niemieckojęzycznej). Tabela 8 przedstawia fragment ankiety ewidencjonującej zabezpieczenia dla serwera WWW i zawiera listę zabezpieczeń zalecanych, opisanych szczegółowo w odpowiednich rozdziałach katalogu zabezpieczeń. Według takich list, z wykorzystaniem formularzy ustala się, które zabezpieczenia serwer już posiada, które są częściowo obecne, a których nie ma wcale. Ustalana jest w ten sposób lista brakujących zabezpieczeń, szacowany jest ich koszt, podawany priorytet wdrożenia oraz osoba za nie odpowiedzialna. Ze względu na obszerność tych formularzy tabela 8 zawiera tylko specyfikację zalecanych zabezpieczeń. W materiałach pomocniczych OPTI występują ponadto tabele pokazujące zależności między zabezpieczeniami i zagrożeniami. Tabela 8 zawiera listę odnośników do katalogu zabezpieczeń, np. w rozdziale S5.45 można zapoznać się z zabezpieczeniem *„Bezpieczeństwo przeglądarki"*.

Tabela 7

Wykaz zagrożeń dla serwera WWW

Grupa	Numer	Nazwa grupy zagrożeń lub zagrożenia
T2	Grupa	UCHYBIENIA ORGANIZACYJNE
	T2.1	Brak procedur bezpieczeństwa lub niewystarczające procedury
	T2.2	Niewystarczająca wiedza na temat procedur bezpieczeństwa
	T2.4	Niewystarczająca kontrola zabezpieczeń
	T2.7	Nieautoryzowane wykorzystanie praw
	T2.9	Słabe dopasowanie się do zmian w wykorzystaniu środków teleinformatycznych
	T2.28	Naruszenie praw autorskich (nieautoryzowany transfer lub publikacja dokumentów, grafiki lub oprogramowania)
	T2.32	Niewystarczające pasmo przenoszenia (słaba dostępność)
	T2.37	Utrata kontroli na środkami komunikacji (ActiveX, Java)
T3	Grupa	BŁĘDY LUDZKIE
	T3.1	Utrata poufności lub integralności w wyniku błędu ludzkiego
	T3.37	Bezproduktywne poszukiwania internetowe

	T3.38	Błędy konfiguracji i operacji
T4	Grupa	BŁĘDY TECHNICZNE
	T4.10	Skomplikowane formy dostępu do systemu z sieci
	T4.22	Podatności i błędy oprogramowania standardowego
	T4.39	Błędy koncepcyjne oprogramowania
T5	Grupa	DZIAŁANIA ROZMYŚLNE
	T5.2	Manipulowanie danymi lub oprogramowaniem
	T5.19	Nadużycie praw przez użytkownika
	T5.20	Nadużycie praw przez administratora
	T5.21	Koń trojański
	T5.23	Wirusy komputerowe
	T5.28	Przeciążenie (Denial of Sevice)
	T5.43	Makrowirusy
	T5.48	IP Spoofing (węszenie po adresach IP)
	T5.78	DNS Spoofing (węszenie po domenach)
	T5.87	Web spoofing (węszenie po witrynach)
	T5.88	Niewłaściwe użycie aktywnych zawartości

Tabela 8

Wykaz zabezpieczeń dla serwera WWW

Grupa	Numer	Nazwa grupy zabezpieczeń lub zabezpieczenia
S2	Grupa	ORGANIZACJA
	S2.35	Zbieranie informacji o słabościach systemu
	S2.172	Opracowanie projektu stosowania www
	S2.173	Określenie strategii bezpieczeństwa dla www
	S2.174	Zabezpieczenie działania serwera www
	S2.175	Uruchomienie serwera www
	S2.176	Wybór właściwego dostawcy usług internetowych
S3	Grupa	PERSONEL
	S3.4	Szkolenie przed rozpoczęciem eksploatacji oprogramowania
	S3.5	Szkolenie na temat zabezpieczeń
	S3.10	Wybór wiarygodnego administratora i jego zastępców
	S3.11	Szkolenie zespołu administrującego dotyczące utrzymania
S4	Grupa	SPRZĘT I OPROGRAMOWANIE
	S4.33	Używanie programu antywirusowego przy wymianie danych na nośnikach lub za pomocą transmisji
	S4.34	Stosowanie szyfrowania, sum kontrolnych lub podpisów cyfrowych (opcjonalne)
	S4.44	Sprawdzanie obecności makrowirusów w danych przychodzących
	S4.64	Sprawdzanie danych przed ich wysłaniem/ eliminowanie zbędnych informacji
	S4.65	Testowanie nowego sprzętu i oprogramowania
	S4.78	Zachowanie ostrożności przy zmianach konfiguracji
	S4.93	Regularna kontrola integralności
	S4.94	Ochrona plików www
	S4.95	Minimalizacja funkcji systemu operacyjnego
	S4.96	Dezaktywacja DNS
	S4.97	Jedna usługa na jeden serwer
	S4.98	Restrykcyjne ustawienie filtrów pakietów
	S4.94	Ochrona przed modyfikacją informacji
S5	Grupa	KOMUNIKACJA
	S5.45	Bezpieczeństwo przeglądarki
	S5.59	Ochrona przed węszeniem DNS
	S5.64	Secure Shell (opcja)
	S5.65	Stosowanie S-HTTP (opcja)

	S5.66	Stosowanie SSL (opcja)
	S5.69	Ochrona przed aktywnymi zawartościami

Rezultatem procesu kompilacji zamodelowanego systemu jest więc lista zabezpieczeń – wiadomo wówczas, jakie zabezpieczenia są zalecane, jakie już istnieją, a jakie należy dopiero zaimplementować i ile to będzie kosztować. Jeśli w analizowanym systemie pewne zabezpieczenia zostałyby dobrane indywidualnie, posiłkując się analizą ryzyka, to na tym etapie następuje ich konsolidacja z zabezpieczeniami realizującymi ochronę podstawową, przy czym całość procesu wdrażania zarządzania bezpieczeństwem informacji dalej przebiegać już może wg OPTI.

Należy zauważyć, że tworzenie koncepcji bezpieczeństwa systemów teleinformatycznych instytucji jest zagadnieniem bardzo złożonym, mimo że metoda OPTI jest uproszczona i pomija procesy analizy ryzyka tam, gdzie tylko to jest możliwe.

4.2. Wdrożenie zabezpieczeń

Kolejnym etapem wdrażania zarządzania bezpieczeństwem informacji w instytucji [11] jest przygotowanie planu implementacji brakujących zabezpieczeń, uwzględniającego zadania, terminy, nakłady, priorytety oraz osoby odpowiedzialne za ich realizację. Istnieje możliwość oszacowania kosztów zabezpieczeń, więc kierownictwo firmy ma ułatwione zadanie odnosząc się do kwestii związanych z analizą ryzyka, gdyby takowa była prowadzona:

- Czy przewidywany koszt wdrożeń zabezpieczeń stoi w prawidłowej relacji do uzyskanej redukcji ryzyka?
- Czy uzyskany poziom ryzyka szczątkowego jest do zaakceptowania, czy ewentualnie dalej go obniżać, ponosząc przy tym dodatkowe koszty?

4.3. Szkolenia i działania uświadamiające

Należy również opracować plan szkoleń [11] oraz działań uświadamiających z uwzględnieniem hierarchii oraz specyfiki stanowisk pracy. Plan powinien zawierać następującą tematykę:

- cele bezpieczeństwa i zasady polityki obowiązujące w instytucji,
- powody, dla których bezpieczeństwo jest tak ważne dla firmy,
- zakres obowiązków, opis stanowisk oraz procedur związanych z bezpieczeństwem,
- omówienie rezultatów analiz przy określaniu wymagań ochronnych,
- plan wdrożenia i weryfikacji zabezpieczeń,

- skutki zdarzeń wpływających negatywnie na bezpieczeństwo z punktu widzenia użytkowników i całej instytucji,
- konieczność raportowania przypadków naruszeń,
- konsekwencje grożące osobom nie stosującym się do zasad nakreślonych w dokumencie polityki bezpieczeństwa.

Szkolenia należy powtarzać cyklicznie. Obowiązkowo należy też szkolić nowo przyjętych, a także pracowników przesuniętych na inne stanowiska.

4.4. Utrzymywanie osiągniętego i adekwatnego dla instytucji poziomu bezpieczeństwa

Wdrożenie zabezpieczeń oraz przeprowadzenie wspomnianych szkoleń pozwala na osiągnięcie zakładanego poziomu bezpieczeństwa. Bezpieczeństwo jednak nie jest nikomu dane raz na zawsze – wymaga ciągłej troski o jego utrzymywanie. Do podstawowych grup zadań z tego zakresu należą:

- monitorowanie skuteczności zabezpieczeń,
- monitorowanie realizacji założonych celów bezpieczeństwa, zwłaszcza gdy w systemie wprowadza się zmiany,
- audyty kontrolne, rewizje,
- reakcje na incydenty.

5. Wnioski i uwagi końcowe

Należy zwrócić uwagę, że dokument polityki bezpieczeństwa, utworzony na wstępie, przez cały czas życia systemu musi być aktualizowany i dostosowany do pełnionych zadań i zmian zachodzących w środowisku systemu.

Przedstawienie metody ochrony podstawowej teleinformatyki, opisanej na prawie dwóch tysiącach stron, w kilku słowach jest dość trudne, gdyż samo zagadnienie zarządzania bezpieczeństwem informacji posiada złożoną naturę. Prezentowany tu materiał powinien być pomocny przy konstruowaniu swojej polityki bezpieczeństwa i w doborze zabezpieczeń. Szczegółowe informacje są dostępne na witrynie [12].

Oprogramowanie wspomagające cały ten proces [13] jest dostępne w niemieckiej wersji językowej.

LITERATURA

1. ISO/IEC TR 13335-1: 1996, Information technology – Guidelines for the management of IT Security, Part1: Concepts and models for IT Security.
2. ISO/IEC TR 13335-2: 1997, Information technology – Guidelines for the management of IT Security, Part2: Managing and planing IT Security.
3. ISO/IEC TR 13335-3: 1998, Information technology – Guidelines for the management of IT Security, Part3: Techniques for the management of IT Security.
4. ISO/IEC TR 13335-4: 2000, Information technology – Guidelines for the management of IT Security, Part4: Selection of safeguards.
5. ISO/IEC WD 13335-5: 1999, Information technology – Guidelines for the management of IT Security, Part5: Management guidance on Network security.
6. PN-I-13335-1: Technika informatyczna - Wytyczne do zarządzania bezpieczeństwem systemów informatycznych, PKN, styczeń 1999.
7. BS7799 Part 1: Code of practice for Information Security Management, British Standard Institute, 1999.
8. BS7799 Part 2: The Specification for Information Security Management, British Standard Institute, 1999.
9. RFC1244 – Site Security Handbook, Network Working Group, 1991.
10. RFC2196 – Site Security Handbook, Network Working Group, 1997.
11. IT Baseline Protection Manual (IT-Grundschutz Handbuch), version 1999, Bundesamt fuer Sicherheit in der Informationstechnik.
12. www.bsi.de
13. BSI Tool IT Grundschutz, CSC Ploenzke AG, version 2.0, 1999.
14. Muench I.: IT – Grundschutz im Electronic - Commerce, Der Weg zur sicheren Informationstechnik – Aktuelle Beispiele, BSI, 2000.
15. Raport: Przegląd modeli biznesowych, I-Metria S.A., 2000.
16. Trepper Ch.: eCommerce Strategies, Microsoft Press, 2000.
17. Grzywak A., Praca zbiorowa pod redakcją: Bezpieczeństwo systemów komputerowych i telekomunikacyjnych, Materiały Ogólnopolskiej Konferencji NetSec'99, Wydawnictwo SOTEL, Chorzów, 1999.
18. Praca zbiorowa pod redakcją Grzywaka A.: Bezpieczeństwo systemów komputerowych, Wydawnictwo Pracowni Komputerowej Jacka Skalmierskiego, Gliwice, 2000.
19. Grzywak A., Białas A.: Architektura systemów gospodarki elektronicznej - Internet dla giełdy przemysłowej, Materiały Konferencji „Internet w biznesie (B2C)" - Otwock 2000, Wyd. Centrum Promocji Informatyki, 2000.

20. Białas A.: Wybrane problemy bezpieczeństwa w zastosowaniach sieci Internet, Materiały II Ogólnopolskiej Konferencji Internet – Wrocław 2000, Oficyna Wydawnicza Politechniki Wrocławskiej, 2000.
21. Białas A.: Zarządzanie bezpieczeństwem informacji w instytucji na przykładzie ochrony podstawowej – opracowanie polityki bezpieczeństwa, IT Security Magazine, 2000, Nr 12 (16).
22. Białas A.: Zarządzanie bezpieczeństwem informacji w instytucji na przykładzie ochrony podstawowej – przekuwamy politykę bezpieczeństwa w rzeczywistość, IT Security Magazine, 2001, Nr 1 (17).
23. Białas A.: Bezpieczeństwo informacji w systemach gospodarki elektronicznej – przegląd podstawowych problemów, IT Security Magazine, 2001, Nr 2 (18).
24. Białas A.: Wprowadzenie do problematyki zarządzania bezpieczeństwem informacji, NetWorld, 2001, Nr 3.

Recenzent: Prof. dr hab. inż. Andrzej Grzywak

Wpłynęło do Redakcji 13 marca 2001 r.

Abstract

E-commerce systems are very sensitive for IT security problems. Two groups of such problems can be distinguished:

- common for all advanced IT applications,
- specific for e-commerce systems.

Key problems to solve were mentioned:

- internal system security - a base for e-commerce applications,
- electronic transaction security,
- creation of confidence platform for business partners.

IT Security Management approach seems to be obligatory for e-commerce systems. The paper presents all stages (Fig. 1) of IT Baseline Protection methodology, developed by German Federal Agency for Security in Information Technology. An example of fictitious e-commerce system (Fig. 2, Fig. 4.) were used to illustrate:

- creating of IT security policy (Fig. 3 - contents, Tab. 1 - company security objectives, Tab. 2 - B2C subsystem security objectives),
- drawing of IT security concepts

- implementation,
- training and security awareness promotion,
- maintaining of IT security in ongoing operation.

Tab. 3 specifies considered system components, tab. 4 specifies existing and planned applications. Security requirements seems to be high, but baseline control should be useful. Mapping of system was presented (tab. 6) - 25 steps were specified and only one - www server - as an example was shown. Threats considered for this component (tab. 7) and recommended safeguards (tab. 8) realizing baseline protection were specified. The paper discuss possibility of using baseline protection in e-commerce applications.