Marta Woźniak-Zapór

Zarządzanie bezpieczeństwem informacji - metody przeciwdziałania zagrożeniom bezpieczeństwa infromacji na platformie e-learningowej

Bezpieczeństwo : teoria i praktyka : czasopismo Krakowskiej Szkoły Wyższej im. Andrzeja Frycza Modrzewskiego 10/4, 87-97

2016

BEZPIECZEŃSTWO • 2016 nr 4 TEORIA I PRAKTYKA

Marta Woźniak-Zapór

Krakowska Akademia im. Andrzeja Frycza Modrzewskiego

Zarządzanie bezpieczeństwem informacji – metody przeciwdziałania zagrożeniom bezpieczeństwa informacji na platformie e-learningowej

Wprowadzenie

Powołując się na jedną z definicji bezpieczeństwa, odnoszącą się do systemów komputerowych, system taki można uważać za bezpieczny w przypadku, gdy „jego użytkownik może na nim polegać, a zainstalowane oprogramowanie działa zgodnie ze swoją specyfikacją”[1]. Platforma e-learningowa jest systemem, w którym przechowywane są i przetwarzane informacje o różnym charakterze. Są to zarówno materiały dydaktyczne, przeznaczane dla poszczególnych, uprawnionych do ich odczytywania studentów, jak również komponenty, które umożliwiają przechowywanie danych dotyczących indywidualnych osiągnięć dydaktycznych poszczególnych użytkowników. Są to zazwyczaj dane, które nie powinny być udostępniane użytkownikom nieuprawnionym. Z taką sytuacją mamy do czynienia w przypadku np. indywidualnych danych służących do logowania użytkowników do systemu. Podobnie jest w przypadku przeprowadzania egzaminów na platformie e-learningowej. Tutaj także nie powinno dochodzić do nieuprawnionego dostępu do samej treści testu, jak i do wyników egzaminu innych, niż wyniki własnego testu.

W przypadku platformy e-learningowej, podobnie jak w przypadku każdego innego systemu informatycznego, należy przedsięwziąć możliwe środki w celu zapewnienia bezpieczeństwa informacji przechowywanej i przetwarzanej z jej pomocą.

[1] S. Garfinkel, *Practical Unix and Internet Security*, II ed., O’Reilly, 2003.

W związku z tym w dalszej części zostanie podjęta analiza możliwości zabezpieczenia informacji, zarówno pod kątem dostępnych dokumentów zawierających regulacje w zakresie bezpieczeństwa informacji i systemów informatycznych, jak również technicznych możliwości zabezpieczenia samej platformy e-learningowej. Techniczne możliwości zabezpieczenia platformy omówione zostaną na podstawie platformy e-learningowej stosowanej w Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego.

Bezpieczeństwo informacji – bezpieczeństwo systemów informatycznych

Sposoby, zasady i możliwości zapewnienia bezpieczeństwa informacji oraz systemów informatycznych regulowane są ustawami, jak również rozporządzeniami wydawanymi na ich podstawie. Są to m.in. Ustawa o ochronie danych osobowych[2], Ustawa o ochronie danych niejawnych[3], Ustawa o świadczeniu usług drogą elektroniczną[4], Ustawa o ochronie baz danych[5], Ustawa o podpisie elektronicznym[6]. Ponadto stosuje się wytyczne zawarte w normach, m.in. ISO/IEC 27001:2005 – czyli międzynarodowy standard tworzenia Systemów Zrządzania Bezpieczeństwem Informacji, jak również ISO/IEC 17799:2005 (BS 779, PN-ISO/IEC 17779) – informacje dotyczące szczegółowych zaleceń na temat procesu wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji w organizacji, a także ISO/IEC 13335:2000 (PN-I-13335) – zarządzanie bezpieczeństwem informacji w systemach teleinformatycznych[7].

Na ich podstawie, w zależności od rodzaju prowadzonej działalności i charakteru przechowywanych informacji, powinna być tworzona polityka bezpieczeństwa. Dzięki temu możliwe jest uszczegółowienie działań zapewniających bezpieczeństwo przetwarzanych informacji, uniknięcie zachowań mogących doprowadzić do jego naruszenia. Wprowadzenie polityki bezpieczeństwa pozwala również na określenie obszarów dostępu do poszczególnych typów danych oraz zakresów odpowiedzialności za bezpieczeństwo przetwarzanych informacji. Należy pamiętać, że proces zarządzania bezpieczeństwem informacji jest wieloetapowy. Składa się z: planowania, oceny ryzyka, analizy kosztów i zysków, tworzenia strategii bezpieczeństwa, implementacji, jak również audytu systemów informatycznych[8].

---

2 Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 1997 nr 133 poz. 883 z późn. zm.).

3 Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. 2010 nr 182 poz. 1228).

4 Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. 2002 nr 144 poz. 1204 z późn. zm.).

5 Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych (Dz.U. 2001 nr 128 poz. 1402 z późn. zm.).

6 Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (Dz.U. 2001 nr 130 poz. 1450 z późn. zm.).

7 T. Polaczek, *Audyt bezpieczeństwa informacji w praktyce*, Gliwice 2006; A. Białas, *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, wyd. 2, Warszawa 2007.

8 *Administracja i Bezpieczeństwo Systemów Informatycznych.* Prezentacja jest współfinansowana przez Unię Europejską w ramach Europejskiego Funduszu Społecznego w projekcie pt. „Innowacyjna dydaktyka bez ograniczeń – zintegrowany rozwój Politechniki Łódzkiej – zarządzanie Uczelnią, nowo-

Bezpieczeństwo systemów informatycznych[9], zgodnie z normą PN-I-13335[10], określane jest poprzez atrybuty bezpieczeństwa. Do wymienionych atrybutów należą: poufność, autentyczność, dostępność, integralność danych, integralność systemu oraz niezaprzeczalność. Analiza bezpieczeństwa Platformy E-learningowej Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego, zwanej w dalszej części Platformą E-learningową KAAFM, odbędzie się pod kątem technicznym w oparciu o podane atrybuty.

Platforma KAAFM a atrybuty bezpieczeństwa

Pierwszym z wymienionych wcześniej atrybutów bezpieczeństwa była poufność informacji. Może ona być rozumiana jako sytuacja, w której żadna informacja nie zostanie udostępniona, czy też wyjawiona osobom, które nie mają do tego uprawnień. W odniesieniu do Platformy E-learningowej KAAFM wiąże się to z odpowiednimi zapisami w polityce bezpieczeństwa, jak również z zabezpieczeniem dostępu do informacji w aspekcie technicznym. Na platformie znajdują się materiały dydaktyczne, które powinny być udostępnione tylko właściwej grupie studentów. Studentom może także być udostępniony moduł zadaniowy. Polega on na tym, że student w odpowiedzi na zadanie załącza plik ze swoją pracą. Nauczyciel po sprawdzeniu pracy wystawia ocenę lub przesyła stosowną informację dotyczącą poprawy zadania. W takim przypadku student powinien otrzymać jedynie informację skierowaną do niego. Z kolei wyłącznie nauczyciel prowadzący dane zajęcia dydaktyczne powinien mieć możliwość sprawdzenia i oceny zadania, które daje studentom do wykonania. Ponadto w przypadku modułu zadaniowego student może pracować nad zadaniem podłączając na platformie kolejne wersje swojej pracy. Z kolei nauczyciel nie powinien takiej pracy oceniać, dopóki student nie kliknie odpowiedniego przycisku, pozwalającego na przesłanie pracy do oceny. Student powinien mieć pewność, że nikt poza nim nie ma dostępu do jego konta na platformie i nie udostępni niekompletnej pracy do oceny nauczycielowi. Przykład okna z modułem zadaniowym pokazany jest na rysunku 1. Nieuprawniony dostęp do konta studenta, jak również nauczyciela może spowodować naruszenie poufności. Nieupawniony dostęp do konta nauczyciela może spowodować skutki w postaci np. ocen wystawianych studentom za wykonane zadania, błędnych informacji przesyłanych studentom poprzez, dostępne na platformie e-learningowej, możliwości komunikacyjne – mail, czat, forum. Jest to także okazja do uzyskania informacji na temat listy studentów znajdujących się w danej grupie, ich adresów mailowych oraz ocen. Na rysunku 2 pokazano przykład dokumentu pokazującego dostęp do listy, na której odnotowywane są postępy studentów. Nieuprawniony dostęp do konta nauczyciela może spowodować także uzyskanie dostępu do bazy pytań testowych wykorzystywanych np. podczas egzaminowania studentów, czy w testach służących samodzielnej weryfikacji zdobywanej wiedzy.

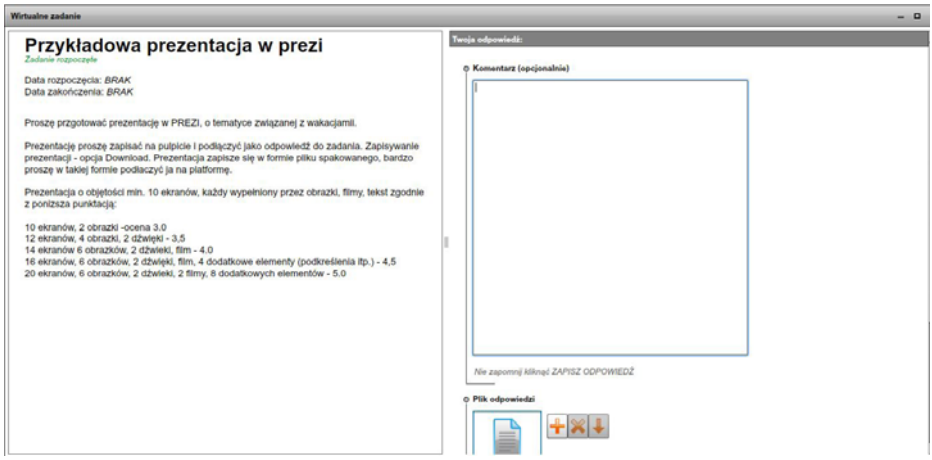
---

czesna oferta edukacyjna i wzmacniania zdolności do zatrudniania osób niepełnosprawnych", http://neo.dmcs.p.lodz.pl/podyplomowe_java/aibss/aibss.pdf [dostęp: 7.07.2016]

9 T. Polaczek, *op. cit.*

10 A. Białas, *op. cit.*

Rysunek 1. Przykład okna z modułem zadaniowym



Źródło: opracowanie własne.

Rysunek 2. Przykład dostępu do listy, na której odnotowane są postępy studentów

Dane osobowe		*Algorytmy i struktury d*
Uzytkownik	**Status**	**Zaliczenie kursu**
Student 1	Trwa	Brak informacji
Student 2		
Student 3		
Student 4		
Student 5	Trwa	Brak informacji
Student 6		
Student 7	Trwa	Brak informacji
Student 8	Trwa	Brak informacji

Źródło: opracowanie własne.

Na Platformie E-learningowej KAAFM, w celu zabezpieczenia poufności danych, stosowany jest system logowania umożliwiający zalogowanie na konto studenta lub nauczyciela z wykorzystaniem indywidualnego loginu i tajnego hasła. Ponadto zarówno nauczyciele, jak i studenci informowani są na szkoleniach o tym, jak ważne jest nieujawnianie danych służących do logowania. Przykład okna logowania pokazany jest na rysunku 3.

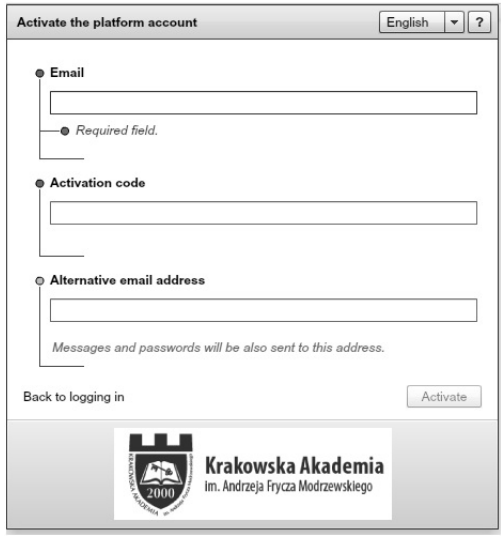
Kolejnym atrybutem bezpieczeństwa jest autentyczność. Przez autentyczność należy rozumieć to, że tożsamość podmiotu lub zasobu pozostaje w zgodzie z podaną deklaracją. W odniesieniu do Platformy E-learningowej KAAFM tożsamość osób biorących udział w zajęciach dydaktycznych, realizowanych na platformie e-lerningowej, weryfikowana jest podczas aktywacji konta. Na tym etapie pracy z wykorzystaniem platformy e-learningowej osoba aktywująca konto zobowiązana jest podać unikatowy klucz, jednoznacznie ją identyfikujący. Dopiero po procesie aktywacji konta

możliwe jest ustawienie hasła logowania do platformy e-learningowej. Przykład okna aktywacji konta pokazany jest na rysunku 4.

Rysunek 3. Okno logowania do platformy e-learningowej

Źródło: opracowanie własne.

Rysunek 4. Okno aktywacji konta na platformie e-learningowej



Źródło: opracowanie własne.

Utrata autentyczności związana z tym, że ktoś inny zaloguje się na konto użytkownika może wynikać z winy samego użytkownika. Dostęp do zasobów platformy e-learningowej możliwy jest po zalogowaniu, informacją tajną podczas logowania jest

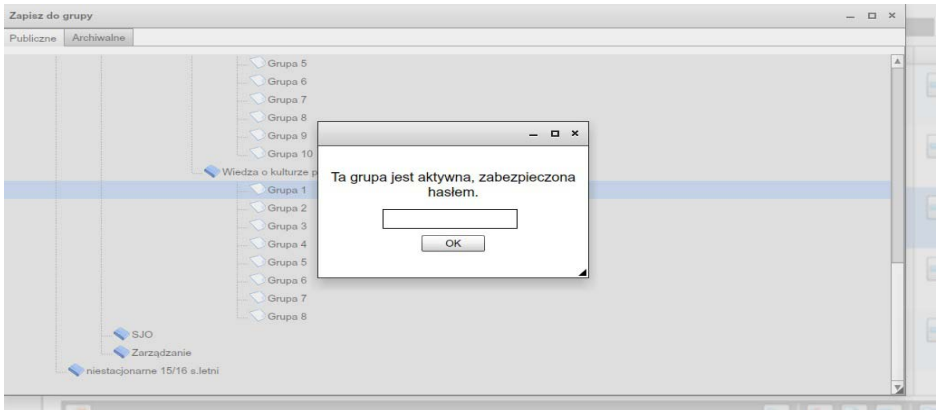
hasło, które oprócz tego, że nie powinno być przekazywane innym użytkownikom, powinno zostać utworzone zgodnie z pewnymi zasadami. Oznacza to, że hasło nie może zawierać znanych i często używanych słów, imion, dat urodzenia czy nazwisk. Każde ustawione hasło, zarówno już podczas aktywacji konta, jak i w przypadku późniejszych jego zmian, nie powinno być w jakikolwiek sposób powiązane z poprzednio ustawionym hasłem. Ponadto po zakończeniu pracy z jakimkolwiek serwisem, do którego uzyskuje się dostęp w wyniku logowania, należy dokonać wylogowania. W przypadku Platformy E-learningowej KAAFM takie wylogowanie następuje automatycznie po upływie zadanego czasu, w którym nie jest widoczna aktywność użytkownika.

Następnym atrybutem bezpieczeństwa jest dostępność. W odniesieniu do platformy e-learningowej może to być odczytywane jako możliwość skorzystania z konkretnych materiałów dydaktycznych w określonym czasie przez osoby do tego uprawnione. Dotyczy to zarówno prowadzonych zajęć dydaktycznych, jak i egzaminów przeprowadzanych z wykorzystaniem platformy e-learningowej. Studenci na Platformie E-learningowej KAFM samodzielnie zapisują się do wirtualnych grup dydaktycznych, których nazwy i miejsce w strukturze zorganizowanej na platformie e-learningowej odpowiadają strukturze uczelni. Stąd też student, chcąc zapisać się do grupy, powinien w strukturze organizacyjnej na platformie e-learningowej zaznaczyć nazwę wydziału, następnie kierunek studiów, przedmiot i dopiero numer grupy dydaktycznej, do której powinien się zapisać. Z uwagi na wykorzystanie platformy e-learningowej do realizacji części zajęć dydaktycznych, grupy na platformie są odpowiednikami grup prowadzonych w formie tradycyjnej, czyli osoba, która uczęszcza do grupy dydaktycznej o określonym numerze, powinna być zapisana do grupy o tym samym numerze na platformie. Studenci w grupie dydaktycznej mogą korzystać z materiałów dydaktycznych udostępnionych dla nich w postaci interaktywnego kursu, załączników z informacjami do przeczytania, zadań, także z dostępnych w ramach grupy możliwości komunikacji – forum, czat, wiadomości. Dlatego ważne jest, aby dostęp do tych zasobów miały osoby, które powinny go mieć. Dostęp taki możliwy jest w terminach wyznaczonych przez nauczyciela, który ma możliwość ustawienia dat dostępu do poszczególnych zasobów i w ten sposób kierować tempem pracy studentów. W celu zabezpieczenia dostępu do grupy, a tym samym zabezpieczenia dostępności informacji dla uprawnionych osób, możliwe jest kodowanie zapisu do grupy hasłem. Oznacza to, że podczas próby zapisu do grupy należy podać hasło, które udostępnia nauczyciel jedynie studentom, którzy powinni się do niej zapisać. Możliwość zabezpieczenia zapisu do grupy hasłem jest także wykorzystywana w czasie egzaminów prowadzonych z wykorzystaniem platformy e-learningowej. Egzaminy odbywają się w salach komputerowych, a studenci mogą się zapisać do danej grupy egzaminacyjnej jedynie przez kilka minut, podczas których grupa jest otwarta do zapisu po wpisaniu hasła, udostępnionego studentom w trakcie wskazanego procesu. Możliwość zapisu do grupy na podstawie wprowadzonego hasła widoczna jest na rysunku 5.

Atrybut dostępności oznacza także zabezpieczenie przed utratą danych, mogącą wystąpić na skutek m.in. awarii sprzętu, czy błędów w oprogramowaniu. Tego typu zagrożenie wymaga działań polegających przede wszystkim na tworzeniu kopii zapasowych zgromadzonych danych oraz zapewnieniu archiwizacji w miejscu innym niż miejsce umieszczenia samego systemu. W odniesieniu do platformy e-learningowej

zabezpieczenia dostępności informacji wiążą się także z zapewnieniem ciągłości zasilania sprzętu umożliwiającego prowadzenie usług sieciowych.

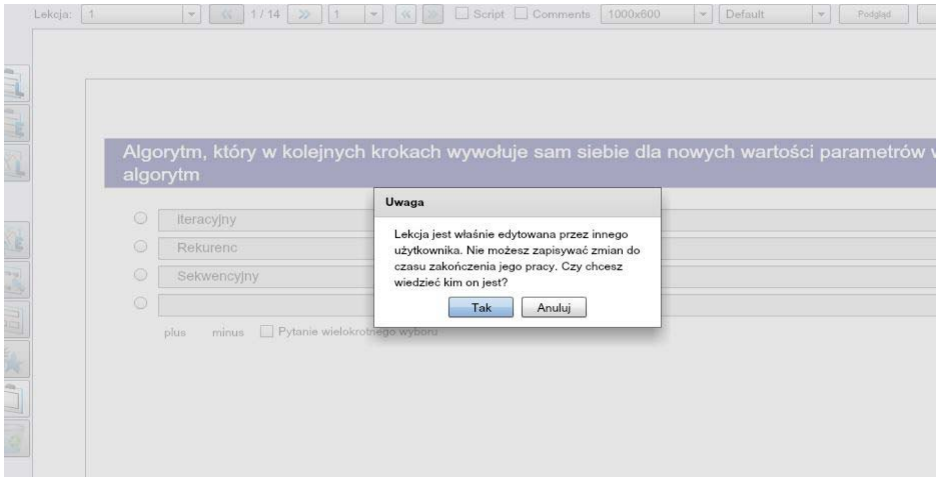
Rysunek 5. Okno zapisu do grupy na podstawie wprowadzonego hasła



Źródło: opracowanie własne.

Jednym z atrybutów bezpieczeństwa jest także integralność. Może ona być rozpatrywana w aspekcie integralności danych i systemu. Integralność systemowa oznacza pracę systemu zgodnie ze swoim przeznaczeniem, bez nieuprawnionej ingerencji. W przypadku Platformy E-learningowej KAAFM dostęp do systemu ma jedynie administrator. Integralność danych rozumiana jest jako sytuacja, w której dane i informacje nie mogą być zmienione i zniszczone w sposób nieautoryzowany oraz nieuprawniony. Możliwość naruszenia informacji jest jednym z istotnych zagrożeń dotyczących platformy e-learningowej. Nie zawsze modyfikacja danych związana jest z działaniem celowym, zdarza się, że jest to działanie wynikające z nieuwagi, zdarzenia przypadkowego. Możliwe jest zapobieganie takim zdarzeniom polegające na kontrolowanym dostępie do informacji zawartych na platformie, w szczególności w tych miejscach, gdzie przypadkowa lub celowo szkodliwa zmiana informacji może mieć poważne skutki. W przypadku dostępu na poziomie nauczyciela, zagrożenia dotyczące naruszenia integralności zaistnieć mogą podczas współtworzenia kursów, udostępniania treści dydaktycznych podczas wspólnej pracy, w ramach prowadzenia jednej grupy dydaktycznej, oraz w trakcie korzystania z bazy pytań testowych. Współtworzenie kursu przez grupę nauczycieli polega na możliwości modyfikowania informacji w projektowanym kursie interaktywnym, ale z pewnymi prawami dostępu. Jedna osoba jest właścicielem kursu i to ona nadaje uprawnienia do jego modyfikowania. Jedynie osoba będąca właścicielem kursu może go usunąć, pozostałe osoby jedynie modyfikować treść. Niebezpieczeństwo tkwi również w jednoczesnym modyfikowaniu treści przez kilka osób. Dlatego zostało wprowadzone zabezpieczenie w postaci stosownej informacji. Użytkownikom, którzy chcieliby zmodyfikować treści w kursie, nad którym w tej samej chwili pracuje inna osoba, zostanie wyświetlona informacja o tym, że kurs jest modyfikowany i nie powinni wprowadzać zmian, ponieważ nie zostaną one zapisane. Na rysunku 6 pokazane zostało okno z zabezpieczeniem przed jednoczesnym wprowadzaniem modyfikacji przez kilka osób.

Rysunek 6. Okno z zabezpieczeniem przed jednoczesnym wprowadzaniem modyfikacji przez kilka osób



Źródło: opracowanie własne.

Możliwość usunięcia lub modyfikacji materiałów dydaktycznych możliwe jest także w przypadku, gdy grupa dydaktyczna prowadzona jest w ramach jednego przedmiotu przez dwóch lub więcej prowadzących. Każdy z nauczycieli widzi materiały dydaktyczne, które są udostępnione w ramach grupy na platformie i może nimi zarządzać tak samo, jak i materiałami, które sam na platformie umieszcza. Zagrożenie może polegać na przypadkowym usunięciu kursu lub innych zasobów udostępnionych przez osobę współprowadzącą zajęcia dydaktyczne. Dlatego pomimo możliwości prowadzenia grup wspólnie przez kilku nauczycieli, ze względów bezpieczeństwa w zakresie integralności danych, grupy prowadzone są zazwyczaj przez jednego prowadzącego.

Znacznym zagrożeniem związanym z możliwością szkodliwej modyfikacji danych jest dostęp do bazy pytań testowych. Baza pytań testowych jest narzędziem wspomagającym i ułatwiającym pracę nauczycieli w zakresie weryfikacji wiedzy. Możliwość ciągłej rozbudowy i dzielenia pytań na kategorie sprawia, że testy, w których jest ona wykorzystywana, mogą w obiektywny sposób sprawdzić wiedzę studentów. Z perspektywy samej bazy pytań i możliwości jej rozbudowy większa liczba nauczycieli pracujących nad dodawaniem kolejnych pytań wpływa korzystnie na zwiększenie puli pytań, z których część losowana wyświetlona zostanie w czasie egzaminu. Z drugiej strony im więcej osób ma dostęp do jednej bazy, tym większe staje się prawdopodobieństwo przypadkowej modyfikacji pytań. W przypadku bazy pytań testowych, podobnie jak w przypadku tworzenia kursu w generatorze, jedna osoba jest właścicielem bazy, a pozostałym osobom współtworzącym taką bazę nadawane jest do tego uprawnienie. Zmniejszenie ryzyka naruszenia integralności odbywać się może w tym przypadku jedynie poprzez kontrolowanie osób, którym zostaje nadany dostęp do bazy pytań testowych i weryfikację ich umiejętności w zakresie jej obsługi.

Atrybutem bezpieczeństwa jest także niezaprzeczalność. Niezaprzeczalność oznacza brak możliwości zaprzeczenia swojemu uczestnictwu w wymianie danych, zarówno części, jak i całości przez jeden z podmiotów uczestniczących w takiej wymianie. Do wymiany danych, w przypadku korzystania z Platformy E-learningowej KAAFM, dochodzi między studentem a nauczycielem w formie komunikatów i informacji przekazywanych w formie czatu, forum i wiadomości. Wiadomości wysyłane z wykorzystaniem któregokolwiek z narzędzi komunikacyjnych nie są usuwane, pozostają na stałe na Platformy E-learningowej KAAFM. W przypadku korzystania z kont studenckich możliwe jest odtworzenie kursu interaktywnego, pobranie informacji w formie plików zamieszczonych w ramach grupy dydaktycznej, podjęcie aktywności związanych z zapoznaniem się z treścią zadania i wykonaniem go. Konto nauczyciela pozwala na umieszczanie plików, kursów, zadań, testów w grupie, ich ocenianie i raportowanie. Nauczyciel ma możliwość raportowania części aktywności podjętych przez studenta, np. fakt czy przeczytał on treść zadania, odtworzył kurs interaktywny. Każda aktywność studenta i nauczyciela, łącznie z danymi dotyczącymi logowania, dodatkowo jest możliwa do raportowania z panelu administratora. W związku z tym nie ma możliwości zaprzeczenia wykonania lub braku wykonania poszczególnych, raportowanych aktywności.

Podsumowanie

Bezpieczeństwo informacji, a zwłaszcza bezpieczeństwo systemów informatycznych, to zagadnienie dotyczące także kształcenia na odległość. W zarządzaniu bezpieczeństwem informacji i systemów informatycznych wsparciem są regulacje w postaci ustaw, rozporządzeń, norm i wewnętrznych zarządzeń wewnętrznych przedsiębiorstw, w których konieczne jest zabezpieczenie informacji. Zabezpieczenie informacji możliwe jest przy prawidłowym zdefiniowaniu zagrożeń. A w tym z kolei pomagają definicje atrybutów bezpieczeństwa. Zgodnie z przytoczoną wyżej normą PN-I-13335, do tych atrybutów zaliczyć można poufność, autentyczność, dostępność, integralność danych, integralność systemu oraz niezaprzeczalność. Zagrożeń takich należy szukać m.in. analizując te atrybuty w odniesieniu do systemu informatycznego, o którego bezpieczeństwo należy zadbać. W przypadku korzystania z platformy e-learningowej wiele zagrożeń generują sami użytkownicy. Naruszenie poufności danych, czy ich autentyczności zależy w dużej mierze od tego, czy użytkownicy dbają o zabezpieczenie haseł dostępu do swojego konta w systemie informatycznym. Stosowanie zasad bezpiecznego konstruowania haseł, jak również nieujawnianie haseł dostępu osobom trzecim sprawia, że można być pewnym, iż z systemu nie skorzysta osoba do tego nieuprawniona. W ten sposób można znacznie zminimalizować zagrożenie umyślnego szkodliwego działania nieuprawnionych osób wewnątrz systemu przechowującego informacje. Zabezpieczenie dostępności informacji związane jest z kolei z koniecznością zabezpieczenia zarówno pod katem zagrożeń wynikających z działalności użytkowników, jak i pod kątem awarii sprzętowych. Z jednej strony widoczna jest konieczność zabezpieczenia udostępniania informacji w odpowiednim czasie i właściwej grupie użytkowników. Z drugiej strony dostępność danych może zostać utracona na skutek różnego rodzaju wypadków, m.in. awarii systemu, czy klęsk

żywiołowych. W przypadku platform e-learningowych konieczne jest również zabezpieczenie integralności systemu i danych. Może ono być rozumiane jako umożliwienie dostępu do określonych zasobów ograniczonej liczbie uprawnionych do wprowadzania modyfikacji użytkownikom. Pozostaje jeszcze kwestia niezaprzeczalności. W przypadku systemów wspomagających kształcenie na odległość związana jest z rejestrowaniem działań w ramach systemu poszczególnych użytkowników. Z jednej strony wzmacnia to poczucie odpowiedzialności i zapewnia zwiększenie uwagi użytkowników podczas wykonywania różnych operacji, w ramach prac na platformie e-learningowej. Z drugiej strony, na podstawie raportów z działalności użytkowników, możliwe jest określenie odpowiedzialności za ewentualne szkody.

Zagrożenia bezpieczeństwa związane są z użytkowaniem każdego systemu informatycznego. Platforma, jako system przetwarzający informacje, również nie jest wolna od zagrożeń. W związku z tym należy zdefiniować możliwe do wystąpienia zagrożenia. Na tej podstawie należy wdrożyć odpowiednie procedury, mające na celu zapobieganie zdefiniowanym zagrożeniom.

Zarządzanie bezpieczeństwem informacji – metody przeciwdziałania zagrożeniom bezpieczeństwa informacji na platformie e-learningowej

Streszczenie

Z rozwojem informatyzacji związane są zagrożenia dotyczące bezpieczeństwa informacji. Zagrożenia te można skategoryzować w ramach atrybutów bezpieczeństwa informacji. Pierwszą z nich jest poufność informacji, druga to dostępność informacji, kolejna związana jest z integralnością informacji i systemu. Pozostałe to autentyczność, oraz niezaprzeczalność. Ich naruszenie może wynikać ze zdarzeń o charakterze przypadkowym, jak i z celowego działania ludzi. W opracowaniu przedstawione zostały najważniejsze ustawy oraz normy dotyczące zarządzania bezpieczeństwem informacji i systemów informatycznych. Została także przedstawiona analiza metod przeciwdziałania zagrożeniom wynikającym z korzystania z systemów informatycznych, w przypadku korzystania z platformy e-learningowej Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego, prowadzona w oparciu o atrybuty bezpieczeństwa, a służąca weryfikacji obecnego stanu zabezpieczenia informacji na platformie uczelnianej oraz ewentualnej poprawy bezpieczeństwa informacji na platformie w przyszłości.

Słowa kluczowe: e-learning, bezpieczeństwo informacji, bezpieczeństwo systemów informatycznych, atrybuty bezpieczeństwa

Information Security Management – Methods of Preventing Threats to the Security of Information on E-learning Platforms

Abstract

With the development of computerization there come related threats to information security. These risks can be categorized as pertaining to the attributes of information security. The first of them is the confidentiality of information, the second is the availability of information, and a yet another one is related to the integrity of information and systems. Others include authenticity and non-repudiation. Infringement of any of them may result

from an action of accidental nature or from deliberate actions of people. This paper presents the most important laws and standards on information security management and information systems. It also presents an analysis of how to prevent risks arising from the use of information systems, including the use of the Andrzej Frycz Modrzewski Krakow University e-learning platform. The analysis is based on security attributes, and serves to verify the current state of information security on the e-learning platform of the University, and the possible improvement of information security on the platform in the future.
Key words: e-learning, information security, information security systems, security attributes

Управление информационной безопасностью – методы противодействия угрозам информационной безопасности на платформе электронного обучения
Резюме

Вместе с развитием информатизации растут также угрозы информационной безопасности. Эти угрозы могут быть классифицированы как часть атрибутов информационной безопасности. Первая из них – конфиденциальность информации, вторая – доступность информации, третья – связана с целостностью информации и систем, четвертая – достоверность. Их нарушение может возникнуть в результате событий случайного характера, а также целенаправленных действий людей. В статье представлены наиболее важные законы и нормы в сфере управления информационной безопасностью и информационными системами. Дан также анализ методов противодействия угрозам, связанным с использованием информационных систем на примере использования платформы электронного обучения Краковской академии им. Анджея Фрыча Моджевского.
Ключевые слова: электронное обучение, информационная безопасность, безопасность информационных систем, атрибуты безопасности