Zeszyty Naukowe Wydziału Elektrotechniki i Automatyki Politechniki Gdańskiej Nr 48

III Konferencja

eTechnologie w Kształceniu Inżynierów eTEE'2016

Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie, 11 kwietnia 2016

NAUCZANIE ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI: STANDARDY I SPOSOBY NAUCZANIA

Rafał LESZCZYNA

Politechnika Gdańska, Wydział Zarządzania i Ekonomii
e-mail: rle@zie.pg.gda.pl

Streszczenie: Pracownicy są najważniejszym ogniwem w ochronie informacji wewnątrz organizacji, gdyż to właśnie oni posiadają regularny dostęp do jej zasobów informacyjnych. Fakt ten jest dobrze rozpoznany przez krajowe oraz międzynarodowe instytucje standaryzujące, które w publikowanych normach zalecają kształcenie, szkolenia i podnoszenie świadomości pracowników jako kluczowy element strategii ochrony informacji przedsiębiorstw. W artykule przedstawiono obowiązujące standardy zarządzania bezpieczeństwem informacji i wskazano miejsca, gdzie definiowane są właściwe polityki, role, odpowiedzialności i działania związane z kształceniem i podnoszeniem świadomości. Następnie zaprezentowano przykład realizacji tych zaleceń w postaci włączenia do programu nauczania Wydziału Zarządzania i Ekonomii Politechniki Gdańskiej przedmiotu „Zarządzanie bezpieczeństwem informacji". Opisano też doświadczenia i obserwacje wynikające z prowadzenia przedmiotu.

Słowa kluczowe: bezpieczeństwo informacji, cyberbezpieczeństwo, zarządzanie bezpieczeństwem informacji, standardy, nauczanie, podnoszenie świadomości.

1. WPROWADZENIE

Eksperci zajmujący się bezpieczeństwem informacji podzielają stanowisko, że najbardziej krytycznym ogniwem w ochronie informacji wewnątrz organizacji, są jej pracownicy. Kadra pracownicza ma regularny dostęp do zasobów informacyjnych i albo brakuje jej wiedzy niezbędnej do zabezpieczenia tych zasobów albo przeciwnie – wie jak ominąć środki bezpieczeństwa, co w obu przypadkach prowadzi do tego samego rezultatu, jakim jest narażenie aktywów informacyjnych na zagrożenia [1].

Jednocześnie, w większości organizacji środki finansowe przeznaczone na zapewnianie bezpieczeństwa kieruje się wyłącznie na rozwiązania techniczne. Wynika to z faktu, że metody techniczne są dobrze zdefiniowane (a co za tym idzie – łatwiejsze do zrozumienia) i dają złudzenie, że ich zastosowanie rozwiąże wszystkie problemy bezpieczeństwa. Popularne jest przekonanie, że nabycie programu antywirusowego, zapory ogniowej, czy ochrony przed złośliwym oprogramowaniem jest całkowicie wystarczające do zapewnienia bezpieczeństwa informacji [2].

Takie podejście okazuje się jednak nieskuteczne. Badania pokazują, że pomimo rosnących inwestycji w techniczne środki bezpieczeństwa, liczba włamań zgłaszanych w ciągu roku rośnie. Dodatkowo większość naruszeń bezpieczeństwa spowodowana jest przez osoby z wewnątrz organizacji. Okazuje się, że rozwiązania techniczne nie czynią systemu informacyjnego bardziej bezpiecznym niż działania ludzi, którzy z niego korzystają, bo niewłaściwe praktyki użytkowników są w stanie pokonać nawet najbardziej starannie zaplanowany system zabezpieczeń [2].

Odpowiedzią na te problemy są działania związane z edukacją, szkoleniami i podnoszeniem świadomości wśród pracowników. W ich efekcie, w miejsce dotychczasowej niewielkiej liczby zatrudnionych ekspertów bezpieczeństwa, organizacja, starając się ochronić swoje zasoby informacyjne, zyskuje wsparcie wszystkich pracowników, którzy w wyniku kształcenia stają się świadomi istoty tego działania. Daje to skutek podobny do rozszerzanie działu bezpieczeństwa informacji na całą organizację. Powstaje „ludzka zapora ogniowa[1]", która będzie bardziej efektywna niż jakiekolwiek rozwiązanie techniczne [2].

Znaczenie edukacji, szkoleń i podnoszenia świadomości jest dziś powszechnie uznane w dziedzinie cyberbezpieczeństwa. Odpowiednie wymagania bezpieczeństwa oraz środki kontrole opisane są w większości, jeśli nie we wszystkich standardach bezpieczeństwa. Liczba inicjatyw edukacyjnych rośnie [1, 3].

W artykule zaprezentowano wymagania bezpieczeństwa informacji i środki kontrolne zidentyfikowane w obowiązujących standardach dotyczących bezpieczeństwa informacji, a następnie przedstawiono przykład nauczania zarządzania bezpieczeństwem informacji na Wydziale Zarządzania i Ekonomii Politechniki Gdańskiej.

2. DEFINICJE

Informacja jest zasobem, który jak inne ważne zasoby biznesowe, stanowi wartość dla organizacji i w związku z tym powinien być odpowiednio chroniony. Bezpieczeństwo informatyczne chroni informację przed szeroką gamą zagrożeń w celu zapewnienia ciągłości działalności biznesowej, ograniczenia strat ekonomicznych

[1] Zapora ogniowa – techniczny środek ochrony, którego działanie, w pewnym uproszczeniu, polega na analizowaniu i filtrowaniu danych przychodzących z różnych źródeł sieci i Internetu.

i maksymalizacji zwrotu inwestycji oraz możliwości biznesowych [4].

Najbardziej powszechna definicja określa *bezpieczeństwo informacji* jako zachowanie jej: poufności (ang. *confidentiality*), integralności (ang. *integrity*) i dostępności (ang. *availability*). Przy czym *poufność* dotyczy zagwarantowywania, że informacja jest dostępna wyłącznie dla osób do tego upoważnionych, a *dostępność*, że upoważnieni użytkownicy posiadają dostęp do informacji i powiązanych zasobów, kiedy istnieje taka potrzeba. Natomiast informacja jest *integralna*, gdy: odpowiada rzeczywistości i jest kompletna [5]. Innymi słowy, informacja jest nieuszkodzona, niezniekształcona.

Podnoszenie świadomości bezpieczeństwa to zbiór działań mających na celu promowanie bezpieczeństwa, ustalenie odpowiedzialności oraz dostarczanie pracownikom aktualnych informacji o zagrożeniach i słabościach systemów informacyjnych oraz mających im zapobiec środkach bezpieczeństwa [3]. W efekcie podnoszenia świadomości wszystkie osoby mające dostęp do zasobów informacyjnych są świadome związanych z tym konsekwencji oraz zakresu własnej odpowiedzialności za te zasoby.

Szkolenia z zakresu bezpieczeństwa informacji mają na celu rozwinięcie wiedzy i umiejętności związanych z bezpieczeństwem w ramach kadry organizacji, poprzez wspieranie rozwoju kompetencji i pomaganie personelowi w zrozumieniu i realizowaniu ról oraz funkcji bezpieczeństwa. Najważniejsza różnica między szkoleniami a podnoszeniem świadomości polega na tym, że szkolenia mają na celu wykształcenie umiejętności pozwalających wypełniać określoną rolę w organizacji, natomiast podnoszenie świadomości skoncentrowane jest na zwróceniu uwagi konkretnych osób na określone zagadnienie [3].

Szkolenia z uwzględnieniem ról (ang. *role-based training*) bazują na kursach bezpieczeństwa dopasowanych do określonych potrzeb pracowników, których odpowiedzialność za bezpieczeństwo zasobów informacyjnych w organizacji jest znacząca [3].

Edukacja dotycząca bezpieczeństwa informacji to kształcenie specjalistów i profesjonalistów potrafiących projektować nowe rozwiązania bezpieczeństwa oraz podejmować własną inicjatywę. Edukacja integruje umiejętności i kompetencje z różnych obszarów oraz rozszerza je o interdyscyplinarne studium koncepcji, zagadnień i zasad (technologicznych i społecznych). Z założenia edukacja bezpieczeństwa powinna być częścią wyższej edukacji [3].

3. STANDARDY ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

Najważniejszym standardem dotyczącym zarządzania bezpieczeństwem informacji (ZBI) jest norma ISO 27001 i związana z nią rodzina standardów ISO 27000 będącymi fundamentalnymi publikacjami, uznanymi na całym świecie. ISO 27001 jest podstawowym standardem ZBI wdrażanym przez organizacje dowolnej wielkości, działające w różnych branżach, sektorach i dziedzinach gospodarki, czy życia społecznego [6]. Najnowsza wersja standardu to ISO 27001:2013 opublikowana w roku 2013 [7]. W Polsce dostępna jest jego spolszczona wersja – PN-ISO/IEC 27001:2014-12 wydana przez Polski Komitet Normalizacyjny [8].

Kolejną grupą publikacji cieszącą się dużym zainteresowaniem jest rodzina standardów i publikacji specjalnych opracowanych przez Narodowy Instytut Standaryzacji i Technologii (ang. *National Institute of Standards and Technology – NIST*). Publikacje te są odpowiedzią na ogłoszenie w 2002 r. w Stanach Zjednoczonych Aktu Zarządzania Bezpieczeństwem Informacji Federalnej (ang. *Federal Information Security Management Act – FISMA*), który nakłada na organizacje państwowe obowiązek ochrony informacji [9]. Publikacje i standardy NIST, choć kierowane do amerykańskich organizacji federalnych, są dziś adaptowane i wdrażane przez organizacje i przedsiębiorstwa na całym świecie.

W literaturze wspomina się również o BS7799, BS ISO/IEC17799:2000, GASPP/GAISP oraz SSE-CMM [10]. Przy czym międzynarodowa norma BS ISO/IEC17799:2000 jest bezpośrednią pochodną brytyjskiego BS7799. W roku 2007 została ona zaadaptowana jako ISO/IEC 27002:2005 [4] i od tego czasu należy do rodziny ISO 27000.

Natomiast GASSP/GAISP (ang. *Generally Accepted Systems/Information Security Principles*) i SSE-CMM (ang. *System Security Engineering Capability Maturity Model*) są raczej zbiorami dobrych praktyk dotyczących bezpieczeństwa informacji.

3.1. Rodzina standardów ISO/IEC 27000

Rodzina ISO/IEC 27000, często określana jako "rodzina standardów zarządzania bezpieczeństwem informacji", składa się z norm bezpieczeństwa informacji opracowanych wspólnie przez Międzynarodową Organizację Normalizacyjną (ang. *International Organization for Standardization – ISO*) i Międzynarodową Komisję Elektrotechniczną (ang. *International Electrotechnical Commission – IEC*) [11].

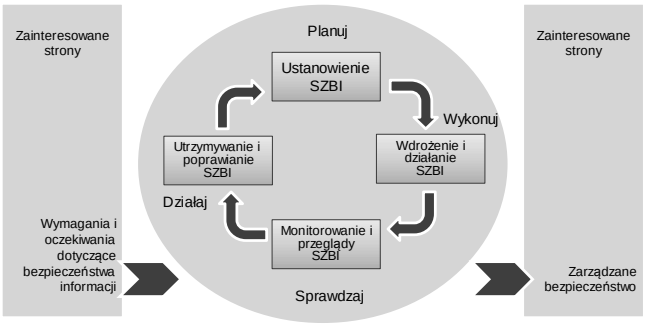
Normy należące do serii ISO/IEC 27000 przedstawiają zalecenia dotyczące dobrych praktyk zarządzania bezpieczeństwem informacji w ramach całościowego Systemu Zarządzania Bezpieczeństwem Informacji - SZBI (ang. *Information Security Management System – ISMS*), analogicznego do systemów zarządzania wykorzystywanych w zapewnianiu jakości (rodzina ISO 9000), czy ochronie środowiska (ISO 14000) [11].

Zakres tematyczny norm jest szeroki i wykracza poza typowe zagadnienia prywatności, poufności, czy technicznych aspektów bezpieczeństwa. Poruszane są obszary bezpieczeństwa fizycznego, osobowego, teleinformatycznego oraz prawnego. Wskazano obszary, które powinny zostać poddane uregulowaniom prawnym.

Zalecenia przedstawione w normach definiowane są w sposób na tyle ogólny, że można je zastosować w organizacjach o dowolnym profilu działalności i dowolnej wielkości. Z tego samego powodu w standardach nie podaje się szczegółowych technicznych wymagań. Organizacje zachęcane są do oceny ryzyka bezpieczeństwa informacji, a następnie do wdrożenia odpowiednich środków kontrolnych wykorzystując normy w zakresie zależnym od potrzeb.

Jak wspomniano wcześniej, sztandarową normą z rodziny ISO/IEC 27000 jest ISO/IEC 27001, gdzie przedstawiono specyfikację Systemu Zarządzania Bezpieczeństwem Informacji (SZBI). System ten oparty jest na podejściu procesowym zgodnie z cyklem Deminga – Planuj–Wykonuj–Sprawdzaj–Działaj (ang. *Plan–Do–Check-Act – PDCA*) przedstawionym na rysunku 1. Podstawą ustanowienia oraz utrzymania SZBI jest określenie metody oraz przeprowadzenie analizy ryzyka. W normie

zdefiniowano cele stosowania zabezpieczeń i zabezpieczenia związane z ustanowieniem, wdrożeniem, eksploatacją, monitorowaniem, przeglądem, utrzymaniem i doskonaleniem SZBI. Kluczowym komponentem standardu jest określenie środków kontrolnych związanych z ustanowieniem i zarządzaniem SZBI, dokumentacją, odpowiedzialnością kierownictwa, wewnętrznymi audytami SZBI, przeglądami SZBI oraz ciągłym doskonaleniem SZBI. Aktualna wersja normy opisuje 114 zabezpieczeń zgrupowanych w 14 obszarach oraz podaje 35 celów stosowania zabezpieczeń i kategorii bezpieczeństwa. Sam sposób wybierania zabezpieczeń zależny jest od organizacji i powinien być oparty na analizie ryzyka. Wyczerpujący charakter normy pozwala budować SZBI w organizacjach różnej wielkości i z różnych sektorów branżowych. Wdrożone SZBI poddawane są certyfikacji [12].



Rys. 1. Model PDCA zastosowany do procesów SZBI. Źródło: opracowanie własne na podstawie [13]

Certyfikacja polega na przeprowadzeniu zewnętrznego audytu Systemu Zarządzania Bezpieczeństwem Informacji. Realizuje się ją etapami w ramach których dokonywana jest ocena dokumentacji SZBI, przeprowadzane są wywiady dotyczące funkcjonowania systemu w praktyce oraz oceniane jest wdrożenie i skuteczność wybranych zabezpieczeń. W etapie końcowym sporządzane są raporty z audytów, które następnie poddawane są weryfikacji pod względem zakresu i kompletności oceny oraz kwalifikacji audytora. Na tej podstawie podejmowana jest decyzja odnośnie przyznania certyfikatu.

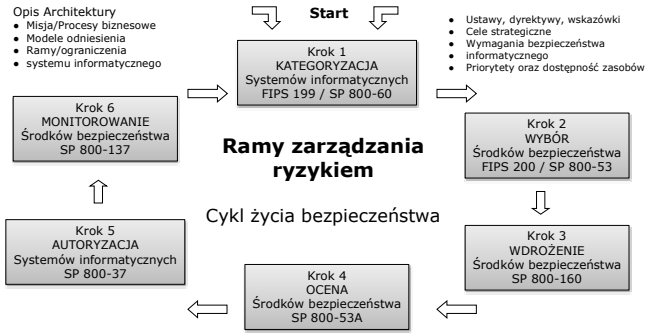
Certyfikat jest ważny przez trzy lata. W okresie tym przeprowadzane są periodyczne (zazwyczaj coroczne, lub co-sześciomiesięczne) audyty nadzoru. Po upływie trzech lat należy wykonać audyt wznawiający (tzw. *recertyfikację*), mający na celu odnowienie certyfikatu.

Certyfikację może przeprowadzić dowolna akredytowana organizacja certyfikująca. Organizacja akredytowana to taka której kompetencje w zakresie przeprowadzania certyfikacji zostały potwierdzone. Przykładowe akredytowane jednostki certyfikacyjne działające w Polsce to (w kolejności alfabetycznej): BSI, DNV, ISOQAR, KEMA, TUV Nord, SGS Group.

Certyfikat ISO 27001 jest potwierdzeniem efektywnego wdrożenia i utrzymywania Systemu Zarządzania Bezpieczeństwem Informacji i stanowi gwarancję zachowania bezpieczeństwa danych organizacji oraz jej klientów. Jego uzyskanie skutkuje podniesieniem wiarygodności organizacji i daje zapewnienie, że powierzone dane są w odpowiedni sposób chronione a zarządzanie ich bezpieczeństwem odbywa się w sposób systematyczny i sformalizowany. Certyfikat stanowi również potwierdzenie, że spełnione są wymogi prawne dotyczące bezpiecznego przetwarzania informacji. W efekcie organizacja zwiększa szanse pozyskania nowych rynków i klientów, otwierając drogę do odbiorców dla których spełnienie określonych norm jest podstawowym warunkiem do rozpoczęcia współpracy.

3.2. Publikacje NIST

W odpowiedzi na wcześniej wspomniany Akt Zarządzania Bezpieczeństwem Informacji Federalnej – FISMA, nakładający na organizacje federalne obowiązek ochrony informacji, NIST opublikowało dwa standardy (FIPS 199 i FIPS 200) oraz szereg tzw. Publikacji Specjalnych (ang. Special Publications), które ze względu na swoje powszechne wykorzystanie nie tylko w Stanach Zjednoczonych, stały się również (de facto) standardami. Publikacje te usytuowane są w tzw. Ramach Zarządzania Ryzykiem (rys. 2). [9]



Rys. 2. Cykl życia bezpieczeństwa informacji w publikacjach NIST. Źródło: opracowanie własne na podstawie [14]

Zasadniczym dokumentem dotyczącym zarządzania bezpieczeństwem informacji jest NIST SP 800-53. Ta Publikacja Specjalna dostarcza wytyczne do wybierania i specyfikowania mechanizmów bezpieczeństwa (ang. *security controls*) dla systemów informatycznych agencji federalnych. Wytyczne dotyczą wszystkich komponentów systemów informatycznych, które przetwarzają, przechowują, bądź transmitują informację federalną [14]. Wytyczne zostały opracowane, aby pomóc we wzmocnieniu bezpieczeństwa systemów informatycznych oraz wspomóc efektywne zarządzanie ryzykiem poprzez:

- zapewnienie zaleceń dotyczących minimalnego zbioru zabezpieczeń, które zapewnią wymagany poziom bezpieczeństwa,
- określenie stabilnego i elastycznego katalogu środków bezpieczeństwa dla systemów informatycznych i organizacji spełniającego współczesne wymagania dotyczące ochrony bezpieczeństwa informacji a także przyszłe wymagania bezpieczeństwa,
- zapewnienie podstawy do prac nad rozwojem metod i procedur oceny efektywności komponentów bezpieczeństwa.

Standard NIST SP 800-53 definiuje komponenty bezpieczeństwa dla trzech poziomów odpowiadających kolejno: systemom i instytucjom o niskiej newralgiczności; systemom i instytucjom o umiarkowanej newralgiczności oraz systemom i instytucjom o wysokiej newralgiczności. Każdy kolejny poziom jest rozszerzeniem poprzedniego.

W publikacji przedstawiono wyczerpującą listę komponentów bezpieczeństwa IT, obejmującą wszelkie obszary zarządzania bezpieczeństwem systemu informatycznego organizacji. NIST SP 800-53 bardzo racjonalnie odnosi się do zagadnień bezpieczeństwa, przedstawiając wymagania możliwe do spełnienia przez

różne organizacje, a jednocześnie wystarczające do zapewnienia dobrego poziomu bezpieczeństwa organizacji. To pewnie z tego powodu, publikacja, pomimo że z założenia dedykowana była amerykańskim agencjom federalnym, znajduje uznanie na całym świecie.

4. EDUKACJA, SZKOLENIA I PODNOSZENIE ŚWIADOMOŚCI W STANDARDACH ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

Wszystkie wymienione wcześniej standardy i publikacje podkreślają znaczenie działań związanych z edukacją, szkoleniami, czy podnoszeniem świadomości użytkowników. Poniżej przedstawiono wymagania, bądź środki kontrolne dotyczące działalności edukacyjnej, szkoleniowej, czy podnoszenia świadomości w standardach bezpieczeństwa ISO/IEC i NIST.

4.1. ISO/IEC 27001 i 27002

Zabezpieczenie A.7.2.2 ("Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji") zdefiniowane w normie ISO/IEC 27001 nakłada na organizacje obowiązek kształcenia oraz przeprowadzania szkoleń i działań uświadamiających wszystkich pracowników, a w szczególnych przypadkach także kontrahentów i (kluczowych) użytkowników zewnętrznych. Powinni oni również regularnie otrzymywać aktualizacje polityk i procedur związanych ze stanowiskiem pracy.

Standard ISO/IEC 27002 zawiera dodatkowe wskazówki dotyczące sposobu wprowadzenia zabezpieczenia A.7.2.2. Zgodnie z nimi, podnoszenie świadomości powinno rozpoczynać się od formalnego wprowadzenia polityk i procedur organizacyjnych oraz od przedstawienia oczekiwań organizacji odnośnie poziomu bezpieczeństwa jej zasobów informacyjnych. Dopiero po tym wprowadzeniu można udzielić pracownikowi dostępu do zasobów informacyjnych organizacji.

Szkolenia powinny dotyczyć wymagań bezpieczeństwa, odpowiedzialności prawnej, czy środków biznesowych, a także poprawnego korzystania z mechanizmów przetwarzania informacji. Podczas szkoleń przedstawia się informacje i dobre praktyki związane z procedurami logowania, korzystaniem z oprogramowania. Szkolenia powinny również podejmować temat postępowania dyscyplinarnego w razie rażącego naruszenia procedur bezpieczeństwa..

Celem podnoszenia świadomości jest wykształcenie wśród pracowników umiejętności samodzielnego rozpoznawania incydentów bezpieczeństwa informacji a następnie reagowania na nie stosownie do roli w organizacji. Przekazywane w ramach podnoszenia świadomości informacje powinny zawierać m.in. charakterystyki znanych zagrożeń, dane osoby kontaktowej w razie wystąpienia incydentu bezpieczeństwa oraz dostępne kanały komunikacyjne.

4.2. NIST SP 800-53

W publikacji NIST SP 800-53 w ramach rodziny AT – "Świadomość i szkolenia" (ang. „*Awareness and Training"*) zdefiniowano cztery środki kontrolne zalecające prowadzenie następujących działań:

1. Tworzenie, dokumentowanie i upowszechnianie polityk i procedur dotyczących szkoleń i podnoszenia świadomości w dziedzinie bezpieczeństwa.
2. Szkolenie użytkowników systemu informacyjnego (w tym członków zarządu, kadry kierowniczej i kontrahentów) w ramach wstępnego szkolenia dla nowych użytkowników, a następnie okresowo.
3. Przeprowadzenie szkolenia opartego na rolach dla personelu z przypisanymi rolami bezpieczeństwa i odpowiedzialnościami – przed zezwoleniem na dostęp do systemu informatycznego lub wykonywania powierzonych obowiązków, a następnie okresowo.
4. Dokumentowanie i monitorowanie szkoleń bezpieczeństwa informacji przebytych przez pracowników organizacji i zarządzanie dziennikiem szkoleń.

Definicja każdego ze środków zawiera dokładny opis, informacje dodatkowe a także możliwe rozszerzenia (jeśli dostępne).

Poza rodziną AT, w NIST SP 800-53 definiuje się także inne środki kontrolne poruszające zagadnienia edukacji, szkoleń i podnoszenia świadomości w dziedzinie bezpieczeństwa.

PM-13 „Pracownicy bezpieczeństwo informacji" (ang. „*Information security workforce*") wymaga ustanowienia programu rozwoju i kształcenia pracowników w zakresie bezpieczeństwa informacji.

PM-14 „Testowanie, szkolenia i monitorowanie" (ang. „*Testing, trainig and monitoring*") kładzie nacisk na przeprowadzanie w ramach organizacji oraz koordynowanie testów, szkoleń i monitorowania z zakresu bezpieczeństwa. Informacją wejściową dla tych działań powinny być wyniki aktualnie przeprowadzonych ocen zagrożeń i podatności systemu informacyjnego organizacji.

CP-3 „Przygotowanie na nieprzewidziane zdarzenia" (ang. „*Contingency training*") i IR-2 "Szkolenia z reagowania na incydenty" (ang. "*Incident response training*") nakładają na organizacje wymóg przeprowadzania szkoleń dotyczących gotowości na nieprzewidziane incydenty bezpieczeństwa oraz sposobów reagowania na nie.

SA-16 "Szkolenia przeprowadzone przez twórców oprogramowania" (ang. "*Developer-provided training*") zaleca przeprowadzanie szkoleń dla użytkowników systemu prowadzonych przez jego twórców, z zakresu prawidłowego korzystania z funkcji i mechanizmów bezpieczeństwa, wbudowanych w oprogramowanie.

5. PRZYKŁAD: NAUCZANIE ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI NA WYDZIALE ZARZĄDZANIA I EKONOMII POLITECHNIKI GDAŃSKIEJ

Rozpoznając znaczenie podnoszenia świadomości w dziedzinie bezpieczeństwa informacji w przedsiębiorstwach i organizacjach, do programu nauczania studentów Wydziału Zarządzania i Ekonomii Politechniki Gdańskiej włączono w roku 2010 przedmiot „Zarządzanie bezpieczeństwem informacji". Celem przedmiotu jest zapoznanie studentów z podstawami i głównymi koncepcjami zarządzania bezpieczeństwem informacji, ze szczególną uwagą poświęconą cyklowi życia zarządzania bezpieczeństwem.

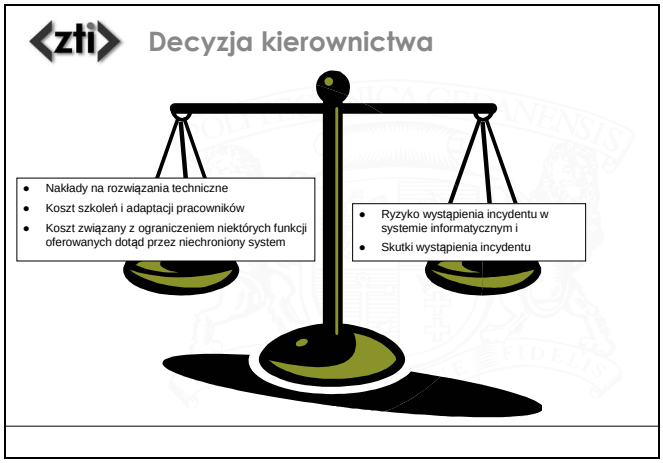
Formuła przedmiotu została opracowana w taki sposób, aby podczas ćwiczeń laboratoryjnych, studenci pracując w grupach, przechodzili przez kolejne etapy cyklu życia zarządzania bezpieczeństwem informacji, począwszy od wyboru przedsiębiorstwa będącego podstawą dalszych analiz, poprzez szacowanie ryzyka i kosztu, kończąc na wyborze właściwych zabezpieczeń i środków kontrolnych

(zarówno technicznych, ale przede wszystkim zarządczych i fizycznych). Zajęcia laboratoryjne poprzedzone są wykładem, którego zadaniem jest dostarczenie wiedzy potrzebnej na laboratorium. Przedmiot składa się z piętnastu godzin wykładu i trzydziestu godzin laboratorium.

5.1. Wykład

Treść wykładu jest następująca:

- Wprowadzenie: kontekst bezpieczeństwa informacji, gospodarka oparta na wiedzy, wzrost liczby i złożoności ataków, problemy i wyzwania bezpieczeństwa, infrastruktury krytyczne, organizacje NIST, ISO i IEC, wymogi prawne, definicje podstawowych pojęć
- Koszt zarządzania bezpieczeństwem informacji w przedsiębiorstwie: uzasadnienie, główne przesłanki w procesie podejmowania decyzji o wprowadzeniu systemu zarządzania bezpieczeństwem informacji przez kierownictwo (rys. 3), zapotrzebowanie na metody oceny kosztów bezpieczeństwa, przegląd istniejących metod
- System Zarządzania Bezpieczeństwem Informacji (SZBI): wyjaśnienie, cykl życia
- Standard ISO/IEC 27001: podstawowe cechy normy, SZBI, model PDCA (cykl Deminga, rys. 1), szczegółowe wytłumaczenie czterech faz cyklu życia SZBI, Załącznik A – cele stosowania zabezpieczeń oraz zabezpieczenia, wyjaśnienie na przykładzie sposobu definiowania zabezpieczeń w normie
- NIST Special Publication 800-53: rodzaje dokumentów NIST (standardy, publikacje specjalne, inne), partnerzy i konsultanci NIST, cele NIST SP 800-53, środki kontrolne, wyjaśnienie na przykładzie sposobu opisu środków kontrolnych w normie, zbiory podstawowe środków, ramy zarządzania bezpieczeństwem (rys. 2), standardy FIPS 199 i 200
- Proces zarządzania bezpieczeństwem informacji zgodny z ISO/IEC 27001 i NIST SP 800-53
- Polityka bezpieczeństwa informacji
- Zagrożenia bezpieczeństwa: opisy i klasyfikacje



Rys. 3. W ramach wykładu wyjaśniane są główne przesłanki w procesie podejmowania decyzji o wprowadzeniu systemu zarządzania bezpieczeństwem informacji przez kierownictwo. Źródło: opracowanie własne

- Zarządzanie ryzykiem: wprowadzenie, podstawowe pojęcia (ryzyko, zagrożenie, podatność itp.), ramy, metodyki i standardy, metody analizy ryzyka, szczegółowe przedstawienie uproszczonej metody jakościowej szacowania ryzyka
- Zabezpieczenia techniczne: zapory ogniowe, kryptografia, identyfikacja i uwierzytelnianie, kontrola dostępu, systemy wykrywania włamań
- Bezpieczeństwo fizyczne, bezpieczeństwo pracowników, szkolenia i podnoszenie świadomości

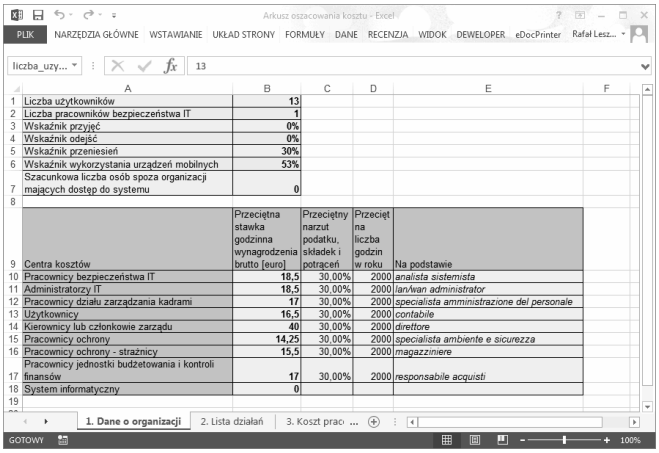
5.2. Laboratorium

Praca laboratoryjna stanowi rdzeń przedmiotu zarządzanie bezpieczeństwem informacji. Ćwiczenia prowadzone są równolegle do wykładu, ale z pewnym opóźnieniem, tak, aby studenci zostali wcześniej wprowadzeni do każdego tematu. Jest to możliwe, ponieważ w pierwszym etapie studenci powinni najpierw utworzyć trzyosobowe grupy, a następnie każda z grup wybiera istniejące bądź odpowiednio przygotowane – fikcyjne – przedsiębiorstwo, w odniesieniu do którego będą przeprowadzane dalsze analizy.

Następnie przedsiębiorstwo powinno zostać przeanalizowane z punktu widzenia bezpieczeństwa, aby między innymi umożliwić oszacowanie skutków zagrożeń. Z tego powodu w pierwszej kolejności należy przedstawić i przeanalizować model biznesu oraz funkcjonowanie przedsiębiorstwa, gdyż w zależności od tego, niektóre zasoby informacyjne są bardziej, a inne mniej – ważne. Studenci opisują misję, cele, strukturę organizacyjną oraz główne obszary działalności przedsiębiorstwa. Następnie analizują jego system informacyjny, opisują je i tworzą diagramy. Wyniki umieszczane są w raportach. Ta część wprowadzająca trwa trzy tygodnie (dwie godziny tygodniowo). W międzyczasie studenci uczestniczą w wykładzie na temat zagadnień niezbędnych do przeprowadzenia dalszych studiów (w tym przypadku – szacowania kosztu).

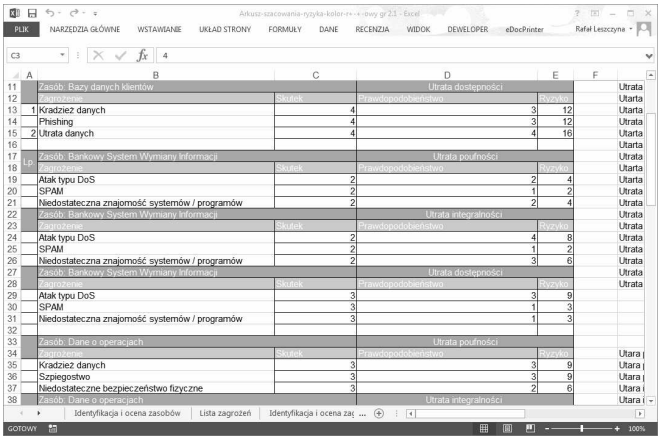
Przez kolejne dwa tygodnie studenci szacują koszt zarządzania bezpieczeństwem informacji w przedsiębiorstwie. W tym celu określają wartości wskaźników charakteryzujących przedsiębiorstwo, takich jak liczba użytkowników, liczba pracowników bezpieczeństwa, czy wskaźnik przyjęć (rys. 4). Następnie wprowadzają te dane do arkusza kalkulacyjnego, aby otrzymać wyniki oszacowań. Wyniki te poddawane są analizie, a wnioski oraz powiązane dane przedstawiane w raporcie.

Następną częścią ćwiczeń laboratoryjnych jest szacowanie ryzyka. Studenci identyfikują zasoby informacyjne w organizacji, opisują je i oceniają skutek naruszeń poufności, integralności i dostępności tych zasobów. Każda grupa studentów analizuje dostępne listy i klasyfikacje zagrożeń bezpieczeństwa informacji i na ich podstawie przygotowuje własną listę zagrożeń adekwatną do ich przedsiębiorstwa. Następnie dla sześciu zasobów, wybranych w oparciu o wcześniej ustalone i uzasadnione kryteria, studenci oceniają prawdopodobieństwa zagrożeń i określają wielkość ryzyka (rys. 5). Jak dla każdego etapu pracy laboratoryjnej, wyniki umieszczane są w raporcie.



	A	B	C	D	E	F
1	Liczba użytkowników	13				
2	Liczba pracowników bezpieczeństwa IT	1				
3	Wskaźnik przyjęć	0%				
4	Wskaźnik odejść	0%				
5	Wskaźnik przeniesień	30%				
6	Wskaźnik wykorzystania urządzeń mobilnych	53%				
7	Szacunkowa liczba osób spoza organizacji mających dostęp do systemu	0				
8						
9	Centra kosztów	Przeciętna stawka godzinna wynagrodzenia brutto [euro]	Przeciętny narzut podatku, składek i potrąceń	Przeciętna liczba godzin w roku	Na podstawie	
10	Pracownicy bezpieczeństwa IT	18,5	30,00%	2000	*analista sistemista*	
11	Administratorzy IT	18,5	30,00%	2000	*lan/wan administrator*	
12	Pracownicy działu zarządzania kadrami	17	30,00%	2000	*specialista amministrazione del personale*	
13	Użytkownicy	16,5	30,00%	2000	*contabile*	
14	Kierownicy lub członkowie zarządu	40	30,00%	2000	*direttore*	
15	Pracownicy ochrony	14,25	30,00%	2000	*specialista ambiente e sicurezza*	
16	Pracownicy ochrony - strażnicy	15,5	30,00%	2000	*magazziniere*	
17	Pracownicy jednostki budżetowania i kontroli finansów	17	30,00%	2000	*responsabile acquisti*	
18	System informatyczny	0				
19						

Rys.4. Szacując koszt bezpieczeństwa informacji studenci wprowadzają do arkusza kalkulacyjnego wskaźniki charakteryzujące przedsiębiorstwo. Źródło: opracowanie własne



	A	B	C	D	E	F	
11		Zasób: Bazy danych klientów		Utrata dostępności			Utrata
12		Zagrożenie	Skutek	Prawdopodobieństwo	Ryzyko		Utrata
13	1	Kradzież danych	4	3	12		Utrata
14		Phishing	4	3	12		Utrata
15	2	Utrata danych	4	4	16		Utrata
16							Utrata
17		Zasób: Bankowy System Wymiany Informacji		Utrata poufności			Utrata
18		Zagrożenie	Skutek	Prawdopodobieństwo	Ryzyko		Utrata
19		Atak typu DoS	2	2	4		Utrata
20		SPAM	2	1	2		Utrata
21		Niedostateczna znajomość systemów / programów	2	2	4		Utrata
22		Zasób: Bankowy System Wymiany Informacji		Utrata integralności			Utrata
23		Zagrożenie	Skutek	Prawdopodobieństwo	Ryzyko		Utrata
24		Atak typu DoS	2	4	8		Utrata
25		SPAM	2	1	2		Utrata
26		Niedostateczna znajomość systemów / programów	2	3	6		Utrata
27		Zasób: Bankowy System Wymiany Informacji		Utrata dostępności			Utrata
28		Zagrożenie	Skutek	Prawdopodobieństwo	Ryzyko		Utrata
29		Atak typu DoS	3	3	9		
30		SPAM	3	1	3		
31		Niedostateczna znajomość systemów / programów	3	1	3		
32							
33		Zasób: Dane o operacjach		Utrata poufności			
34		Zagrożenie	Skutek	Prawdopodobieństwo	Ryzyko		Utrata
35		Kradzież danych	3	3	9		Utrata
36		Szpiegostwo	3	3	9		Utrata
37		Niedostateczne bezpieczeństwo fizyczne	3	2	6		Utrata
38		Zasób: Dane o operacjach		Utrata integralności			Utrata

Rys.5. Określając wartości ryzyka studenci oceniają skutek naruszeń poufności, integralności i dostępności zasobów oraz prawdopodobieństwa zagrożeń. Źródło: opracowanie własne

Kiedy studenci mają świadomość kontekstu bezpieczeństwa ich organizacji, znają możliwe zagrożenia i ich wpływ na działalność biznesową przedsiębiorstwa, oraz potrafią usystematyzować zasoby informacyjne w oparciu o powiązane ryzyka – są gotowi do przygotowania polityki bezpieczeństwa. Wynikowy dokument polityki bezpieczeństwa powinien powstać na bazie wcześniejszych analiz oraz analizy dostępnych publikacji tego typu.

Ćwiczenia laboratoryjne kończą się wyborem zabezpieczeń lub środków kontrolnych zgodnych ISO/IEC 27001 lub NIST SP 800-53. Studenci muszą uzasadnić swój wybór standardu oraz wybrać środki ochrony dla sześciu zasobów informacyjnych wyłonionych w ramach szacowania ryzyka. Następnie opisują te środki, bądź przedstawiają i uzasadniają fakt niewybrania środków z danej kategorii. Każda grupa przygotowuje nowy diagram systemu informacyjnego, uzupełniony o zabezpieczenia techniczne. Na koniec studenci przedstawiają własne wnioski i obserwacje.

Aby zaliczyć przedmiot, studenci powinni uczestniczyć we wszystkich pięciu częściach laboratorium, wykonać związane z nimi prace i przedstawić poprawne raporty. Oprócz tego muszą uzyskać pozytywny wynik ze sprawdzianu wiedzy opartego na pytaniach testowych oraz otwartych.

6. WNIOSKI KOŃCOWE

Rozpoznając kluczową role pracowników w ochronie bezpieczeństwa informacji przedsiębiorstw i organizacji, standardy ISO/IEC 27001 i NIST SP 800-53 zalecają stworzenie programów kształcenia, szkoleń i podnoszenia świadomości w dziedzinie bezpieczeństwa, które definiują właściwe polityki, role, odpowiedzialności i działania. Te ostatnie mogą obejmować bezpośrednią lub pośrednią komunikację oraz działania kierownictwa w celu zwrócenia uwagi pracowników na zagadnienia bezpieczeństwa (podnoszenie świadomości), wykształcenie określonych umiejętności związanych z ochroną informacji (szkolenia), czy też długoterminowe i interdyscyplinarne studia najczęściej prowadzone w szkołach wyższych (edukacja).

Doświadczenia związane z prowadzeniem przedmiotu zarządzanie bezpieczeństwem informacji na Wydziale Zarządzania i Ekonomii Politechniki Gdańskiej wskazują na kluczową rolę zajęć praktycznych w nauczaniu zagadnień związanych z ochroną informacji w organizacjach. Wyniki sprawdzianów wiedzy pokazują, że studenci chętniej odnoszą się do wiedzy oraz doświadczeń uzyskanych podczas pracy w laboratorium, niż do wiedzy teoretycznej przedstawianej na wykładzie. Widać to na podstawie przykładów podawanych przez studentów w celu zilustrowania odpowiedzi. Przedmiot prowadzony jako połączenie zajęć laboratoryjnych z wykładem (z naciskiem na te pierwsze) daje więc większe szanse uzyskania pozytywnych rezultatów ocen wiedzy przyswojonej przez studentów, a co za tym idzie – wyższy poziom świadomości znaczenia zagadnień bezpieczeństwa informacji w przedsiębiorstwach.

Przedmiot zarządzanie bezpieczeństwem informacji został wprowadzony do programu nauczania Wydziału Zarządzania i Ekonomii ponieważ znaczna część jego absolwentów obejmie w przyszłości kierownicze lub administracyjne stanowiska i będzie miało bezpośredni wpływ na kształt cyberbezpieczeństwa w organizacjach. W dzisiejszych czasach, przy powszechnym wykorzystaniu Internetu i systemów informacyjnych przez przedsiębiorstwa oraz lawinowo rosnącej liczbie i złożoności ataków, taki podstawowy kurs powinien być wprowadzony do programów wszystkich szkół wyższych o podobnym profilu.

7. BIBLIOGRAFIA

1. Hight S. D.: The importance of a security, education, training and awareness program, 2005.
2. Motorola: The User Role in Information Security, 2010.
3. Bowen P., Hash J., Wilson M.: NIST SP 800-100 Information Security Handbook: A Guide for Managers, 2006.
4. ISO/IEC: ISO/IEC 27002:2005: Information technology — Security techniques — Code of practice for information security management, 2005.
5. ISO/IEC: ISO/IEC 27005:2011: Information technology — Security techniques — Information security risk management, 2011.
6. Humphreys E.: Information security management system standards, Datenschutz und Datensicherheit - DuD 35, 2011, s. 7–11.

7. ISO/IEC: ISO/IEC 27001:2013: Information technology – Security techniques – Information security management systems – Requirements, http://shop.bsigroup.com/ProductDetail/?pid=000000000030313534, 2013.
8. Polski Komitet Normalizacyjny: PN-ISO/IEC 27001:2014-12: Technika informatyczna — Techniki bezpieczeństwa — Systemy zarządzania bezpieczeństwem informacji — Wymagania, 2014.
9. Ross R., Katzke S., Toth P.: The New Fisma Standards and Guidelines Changing The dynamic of Information Security for the Federal Government. In: MILCOM 2005 - 2005 IEEE Military Communications Conference. pp. 1–7. IEEE 2005.
10. Siponen M., Willison R.: Information security management standards: Problems and solutions, Inf. Manag. 46, 2009, s. 267–270.
11. ENISA: Protecting Industrial Control Systems - Recommendations for Europe and Member States, ENISA 2011.
12. Humphreys E.: Information security management standards: Compliance, governance and risk management, Inf. Secur. Tech. Rep. 13, 2008, s. 247–255.
13. Polski Komitet Normalizacyjny: PN-ISO/IEC 27001:2007: Technika informatyczna — Techniki bezpieczeństwa — Systemy zarządzania bezpieczeństwem informacji — Wymagania, 2007.
14. National Institute of Standards and Technology (NIST): NIST SP 800-53 Rev. 4 Recommended Security Controls for Federal Information Systems and Organizations, U.S. Government Printing Office 2013.

TEACHING INFORMATION SECURITY MANAGEMENT: STANDARDS AND PRACTICE

Security experts agree that people are the critical factor in protection of organisations' cyber assets. The end-users access the assets on a regular basis and in most cases either they lack the security knowledge necessary to protect them or they know how to avoid protection mechanisms – in both cases the result is the same, namely the exposure of the cyber assets to threats.

At the same time the majority of organisations concentrate their information security budget on technical solutions. This is because technical methods are well-defined (thus – comprehensible) and give an illusion that when applied all security issues will be solved. Acquire a "box" – an anti-virus, a firewall or an anti-malware – install it, and consider the problem solved.

This approach tends however to be ineffective. Surveys show that despite the gradually increasing investments in technical controls the number of intrusions reported annually also continues to rise. Interestingly, there are reports claiming that the majority of breaches were caused by insiders. Technical solutions cannot make a network more secure than activities of people who use it, because poor user practices overcome the even the most carefully planned security system.

Educating and raising security awareness among personnel is like expanding the information security department into the whole organisation. Instead of few security experts trying to protect the network, security manager has at his/her support each employee of the organisation taking care of the security interests of the company. This establishes some sort of a "human firewall" that will be very likely more efficient than a technical solution, and in contrast to it, able to recognise unknown, previously undetected threats.

The importance of Security Education, Training and Awareness (SETA) is today widely recognised in the cybersecurity domain. The relevant security requirements and controls are described in majority if not all of security standards. The number of SETA initiatives continues to grow.

In this paper security requirements and controls in the information security management standards are presented, followed by the description of an example of their realisation: teaching information security management at the Faculty of Management and Economics of Gdańsk University of Technology.

Keywords: information security, cybersecurity, information security management, standards, education, awareness raising.