Zeszyty Naukowe Uniwersytet Ekonomiczny w Krakowie

6(978)

ISSN 1898-6447
e-ISSN 2545-3238
Zesz. Nauk. UEK, 2018; 6(978): 205–220
https://doi.org/10.15678/ZNUEK.2018.0978.0612

Jan Madej

Koncepcja dobrej praktyki informatycznej dla sądów powszechnych w zakresie kontroli zabezpieczeń stanowisk i urządzeń komputerowych*

Streszczenie

W artykule przedstawiono koncepcję dobrej praktyki IT z zakresu kontroli zabezpieczeń stanowisk i urządzeń komputerowych za pomocą list audytowych. Koncepcja dobrej praktyki powstała podczas realizacji projektu „PWP Edukacja w dziedzinie zarządzania czasem i kosztami postępowań sądowych – case management" programu operacyjnego „Kapitał ludzki". Projekt ten był jednym z elementów wspierających reformę polskiego wymiaru sprawiedliwości i miał na celu podniesienie efektywności procesu orzecznictwa sądów poprzez skrócenie jego czasu, zmniejszenie kosztów oraz podniesienie kwalifikacji pracowników sądownictwa. Zaprezentowano koncepcję wykorzystania list audytowych do przeprowadzenia kontroli zabezpieczeń systemów informatycznych sądów na poziomie poszczególnych stanowisk i urządzeń komputerowych oraz warunki i tło zaproponowanej praktyki (akty prawne, międzynarodowe normy bezpieczeństwa), cele i korzyści wynikające z jej wdrożenia oraz podstawowe założenia, zakres i funkcje, które powinny być realizowane na różnych poziomach dojrzałości. Na zakończenie przedstawiono wnioski z wdrożenia dobrej praktyki.

Jan Madej, Uniwersytet Ekonomiczny w Krakowie, Wydział Zarządzania, Katedra Informatyki, ul. Rakowicka 27, 31-510 Kraków, e-mail: madejj@uek.krakow.pl

* Artykuł powstał w wyniku prac nad projektem pt. „PWP Edukacja w dziedzinie zarządzania czasem i kosztami postępowań sądowych – case management", nr projektu POKL.05.03.00-00-012/11.

Słowa kluczowe: bezpieczeństwo systemów informatycznych, audyt, listy kontrolne, dobre praktyki informatyczne, wymiar sprawiedliwości, sądy.
Klasyfikacja JEL: M15, K00.

1. Wprowadzenie

W artykule została przedstawiona koncepcja dobrej praktyki z zakresu IT przeznaczona do kontroli zabezpieczeń stanowisk i urządzeń komputerowych za pomocą list audytowych. Koncepcja ta powstała podczas wdrażania pilotażu dobrego zarządzania jednostkami wymiaru sprawiedliwości w ramach projektu „PWP Edukacja w dziedzinie zarządzania czasem i kosztami postępowań sądowych – case management" programu operacyjnego „Kapitał ludzki" (*Badanie ewaluacyjne…* 2015). Autor artykułu wchodził w skład zespołu zajmującego się opracowaniem dobrych praktyk informatycznych, które zostały zaproponowane do wdrożenia w 60 sądach różnych szczebli. Warunki realizacji projektu oraz metodyka projektowania i wdrażania dobrych praktyk z zakresu IT zostały omówione w artykule (Grabowski, Madej i Trąbka 2018).

Celem niniejszego artykułu jest przedstawienie zaproponowanej koncepcji wykorzystania list audytowych do kontroli zabezpieczeń systemów informatycznych sądów na poziomie poszczególnych stanowisk i urządzeń komputerowych. Audyt bezpieczeństwa systemów informatycznych (SI) jest procesem, który służy m.in. do określenia stanu bezpieczeństwa zasobów, badania konfiguracji urządzeń komputerowych, wykrywania naruszeń bezpieczeństwa i pogłębienia wiedzy z tego zakresu. Może być on przeprowadzany z wykorzystaniem różnych narzędzi i metod (Liderman i Patkowski 2003, Davis, Schiller i Wheeler 2011, Landoll 2011). Jednym z nich są listy audytowe (listy kontrolne – *checklist*) wykorzystywane przez różne firmy i organizacje. Narzędzie to jest tak wygodne, a zarazem przydatne, że obecnie w USA funkcjonuje opracowany przez National Institute of Standards and Technology (NIST) rządowy program National Checklist Program (NCP) (https://nvd.nist.gov/ncp/) polegający na udostępnianiu gotowych list kontrolnych do sprawdzania konfiguracji zabezpieczeń systemów operacyjnych i aplikacji (Quinn i in. 2018). Taka praktyka zaproponowana została w ramach realizowanego projektu. Należy podkreślić, że dużym problemem wdrożeniowym (a równocześnie ciekawym problemem badawczym) było wdrożenie rozwiązań z obszaru biznesu w tak nietypowej organizacji, jaką jest sąd. Ma to duże znaczenie dla zrozumienia warunków, w których tworzone były praktyki.

Liczne regulacje prawne, którym podlegają sądy, duże znaczenie formalnej i nieformalnej struktury zależności oraz niezawisłość sędziowska czynią z sądów bardzo specyficzne organizacje odbiegające swą strukturą od organizacji funkcjonujących w biznesie. Wizyty w sądach wykazały bardzo zróżnicowany

poziom ich informatyzacji oraz ujawniły wiele trudności z bezpośrednim zastosowaniem rozwiązań informatycznych wykorzystywanych powszechnie. Dobór praktyk utrudniały także często rozbieżne oczekiwania prezesów i dyrektorów sądów co do potrzeby i charakteru informatyzacji tych jednostek. Zdarzało się, że ich stanowisko pozostawało niezmienne pomimo wskazywanych przez zespół dużych możliwości wykorzystania IT w działalności sądów. Członkowie zespołu postanowili zatem wykorzystać metodę badawczą *action research* (AR) i zamiast zaproponowania gotowych rozwiązań informatycznych skupili się na zrozumieniu sposobu postrzegania sądów oraz rozwiązaniu problemów w taki sposób, jak je postrzegają ich pracownicy. *Action research* wykorzystywane jest w kontekście odkrywania teorii potrzebnej do rozwiązywania problemów praktycznych i pozwala m.in. na lepsze zrozumienie złożonego zjawiska poprzez wspólne (przez badacza i badane podmioty) prowadzenie badań oraz równoczesne rozwiązywanie problemów i zdobywanie wiedzy, którą można natychmiast zastosować[1] (Baskerville i Wood-Harper 1996, Baskerville 1999).

Wykorzystanie *action research* zaowocowało opracowaniem koncepcji praktyk, które powstały we współpracy z pracownikami sądu oraz w wyniku obserwacji stosowanych rozwiązań lub jako bezpośrednia odpowiedź na potrzeby sądów. Okazało się także, że oczekiwania pracowników co do poziomu wdrożenia praktyk są zróżnicowane. W związku z czym pojawiła się potrzeba opracowania kilku poziomów realizacji dobrych praktyk, przy konstruowaniu których zespół wzorował się na koncepcji poziomów dojrzałości systemu (Paulk i in. 1993) i standardzie COBIT (*COBIT 4.1…* 2010).

2. Warunki i tło zaproponowanej praktyki

W Polsce, tak jak w innych krajach, sytuacja w zakresie bezpieczeństwa systemów informatycznych jest pochodną obowiązujących rozwiązań prawnych, dostępności technologii teleinformatycznych i świadomości użytkowników. Można z całą pewnością stwierdzić, że troska o bezpieczeństwo SI przestała być dobrowolną praktyką, ale stała się koniecznością i obowiązkiem, który nakładają przepisy prawne obligujące do zapewnienia ochrony zgromadzonych danych oraz przewidują odpowiedzialność karną za ich nieprzestrzeganie. W sądach powszechnych obowiązek ochrony informacji wynika m.in. z takich aktów prawnych, jak:

[1] Należy wspomnieć, że chociaż niektórzy naukowcy krytykowali metodę AR za brak rygoru naukowego oraz trudności w rozróżnieniu pomiędzy nią a konsultingiem (Davison, Martinsons i Kock 2004), to okazała się ona skuteczna w dyscyplinie systemów informacyjnych i obecnie – obok studiów przypadku – należy do głównego nurtu badań w obszarze SI (Cole i Avison 2007).

– Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny,
– Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych,
– Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych,
– Ustawa z dnia 29 września 1994 r. o rachunkowości,
– Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych,
– Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej,
– Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym,
– Ustawa z dnia 5 lipca 2002 r. o ochronie niektórych usług świadczonych drogą elektroniczną opartych lub polegających na dostępie warunkowym,
– Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych,
– Rozporządzenie MSWiA z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych,
– Rozporządzenie Prezesa RM z dnia 20 lipca 2011 r. w sprawie określenia podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych,
– Rozporządzenie RM z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

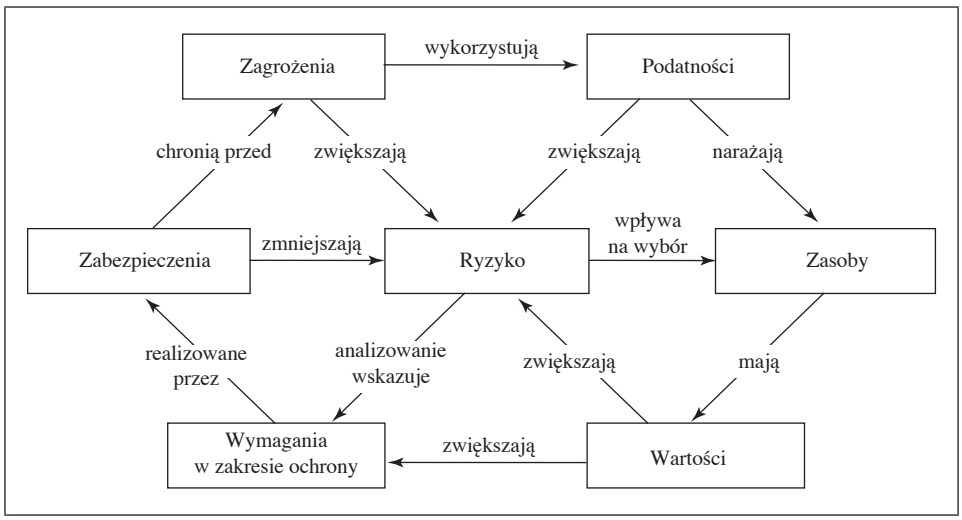
Analiza tych aktów pozwala wyciągnąć wnioski, że przepisy prawa bezwzględnie wymagają zapewnienia kompleksowej ochrony systemów informatycznych, a odpowiedzialność za prawidłową realizację tego zadania ponosi kierownictwo jednostki (Madej 2009). W tej sytuacji znaczenie zyskują sprawdzone rozwiązania określające sposób postępowania pozwalający na osiągnięcie odpowiedniego bezpieczeństwa. Rangę takich rozwiązań mają m.in. normy i standardy z zakresu zarządzania bezpieczeństwem informacji, takie jak:
– PN-ISO/IEC 27001:2007. Systemy zarządzania bezpieczeństwem informacji – Wymagania,
– PN-ISO/IEC 27005. Zarządzanie ryzykiem w bezpieczeństwie informacji,
– PN-ISO/IEC 17799:2007. Praktyczne zasady zarządzania bezpieczeństwem informacji (odpowiednik normy ISO/IEC 27002),
– PN-I-13335-1:1999. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych – Pojęcia i modele bezpieczeństwa systemów informatycznych.

Ich zaletą jest usystematyzowanie wiedzy, zdefiniowanie pojęć i modeli oraz wyróżnienie obszarów ważnych dla bezpieczeństwa, a także określanie wielu szczegółowych wymagań, które należy spełnić, aby osiągnąć zadowalający poziom bezpieczeństwa w SI.

Należy jednak pamiętać, że nawet dysponując odpowiednimi opracowaniami, wiedzą i doświadczeniem, skonstruowanie skutecznego systemu ochrony nie jest

proste. Problematyka bezpieczeństwa jest bardzo rozległa, a główny wpływ na to ma złożona budowa systemów informatycznych oraz zróżnicowanie, duża zmienność i nieprzewidywalny charakter zagrożeń.

Już samo zdefiniowanie pojęcia bezpieczeństwa przysparza wielu problemów, bo chociaż z formalnego punktu widzenia bezpieczeństwo systemu informatycznego to wszystkie aspekty związane z definiowaniem, osiąganiem i utrzymywaniem poufności, integralności, dostępności, rozliczalności, autentyczności i niezawodności systemu (PN-I-13335-1:1999), to na rzeczywiste bezpieczeństwo systemu wpływają takie elementy, jak: zagrożenie, podatność (słabość) zasobu, która może być wykorzystana przez zagrożenie, oraz ryzyko, że zagrożenie wykorzysta podatność zasobu do jego zniszczenia lub wywołania straty. Relacje pomiędzy tymi elementami przedstawiono na rys. 1.



Rys. 1. Relacje między elementami bezpieczeństwa SI

Źródło: opracowanie własne na podstawie (PN-I-13335-1:1999).

Na rys. 1 widoczne są liczne i często złożone relacje, które należy wziąć pod uwagę, analizując zagadnienie związane z bezpieczeństwem SI, tworząc system ochrony, czy wdrażając zabezpieczenia (por. Molski i Łacheta 2006, Polaczek 2006, Liderman 2008). Dlatego mając na uwadze złożoność problemu bezpieczeństwa informatycznego oraz potrzebę i konieczność ochrony SI, zaproponowana została dobra praktyka w zakresie kontroli zabezpieczeń stanowisk i urządzeń komputerowych. Jej prawidłowe wdrożenie wiązało się z poprawą zabezpieczenia systemu ochrony oraz poznaniem relacji pomiędzy poszczególnymi elementami ważnymi z punktu widzenia bezpieczeństwa SI.

3. Cele dobrej praktyki i korzyści wynikające z jej wdrożenia

Zapewnienie bezpieczeństwa sądowych systemów informatycznych, w których – z natury rzeczy – przetwarzane są dane o dużej wrażliwości, jest jednym z podstawowych obowiązków osób zarządzających sądami oraz personelu informatycznego. Dlatego głównym celem proponowanej dobrej praktyki było zwiększenie poziomu bezpieczeństwa systemów informatycznych sądu. Celem pobocznym – ale ważnym z punktu widzenia funkcjonowania SI – było uświadomienie użytkowników w zakresie znaczenia i konieczności dbania o bezpieczeństwo SI. Dobra praktyka została skierowana do wszystkich pracowników sądu, którzy korzystają z jego systemu informatycznego, a za jej wdrożenie odpowiedzialny był dział informatyki.

Należy zaznaczyć, że chociaż w dobrej praktyce chodzi o kontrolę zabezpieczeń stanowisk i urządzeń komputerowych, nie oznacza to, że sprawdzane jest bezpieczeństwo tylko tych elementów. W rzeczywistości jest to kontrola bezpieczeństwa całego systemu informatycznego przez pryzmat stanowisk komputerowych, czyli np. jeżeli na pytanie „czy z twojego komputera (konta, profilu) mogą korzystać pracownicy z innych oddziałów?" odpowiedź jest pozytywna, to może to świadczyć o niewłaściwej konfiguracji sieci komputerowej lub nieprawidłowych rozwiązaniach organizacyjnych w zakresie uprawnień użytkowników w całym systemie. Jak szczegółowo zostanie przeprowadzona kontrola i jakie korzyści przyniesie, zależy tylko od konstrukcji list i rzetelności udzielanych odpowiedzi.

Wspomniany aspekt uświadamiania użytkowników jest pochodną przeprowadzanych kontroli. Regularne kontrole i samokontrole spełniają podstawowe cele szkoleniowe i pozwalają użytkownikom na zapoznanie się m.in. z takimi zagadnieniami, jak: pojęcia związane z bezpieczeństwem SI, potrzeby ochrony i cele polityki bezpieczeństwa SI, funkcjonowanie systemu ochrony, obowiązki i odpowiedzialność użytkowników SI, konsekwencje nieautoryzowanego działania (w tym sankcje dyscyplinarne).

Korzyści z wdrożenia dobrej praktyki mogą być rozpatrywane w trzech aspektach: organizacji pracy, pracownika oraz finansowym. Do korzyści w aspekcie organizacji pracy należy:

– zwiększenie bezpieczeństwa systemu informatycznego,
– identyfikacja mocnych i słabych stron zabezpieczeń SI,
– poprawa funkcjonowania SI,
– zwiększenie możliwości kontroli infrastruktury informatycznej,
– dostosowanie funkcjonowania i zabezpieczania SI do przepisów prawa i norm ISO,
– zmniejszenie liczby sytuacji kryzysowych wynikających z naruszenia bezpieczeństwa systemu.

Do korzyści w aspekcie pracownika należy:
– zwiększenie bezpieczeństwa funkcjonowania stanowiska pracy,
– zwiększenie wiedzy na temat zagadnień związanych z bezpieczeństwem SI,
– zwiększenie świadomości występowania zagrożeń,
– otrzymywanie informacji zwrotnych na temat poziomu zabezpieczeń stanowiska pracy,
– wykorzystanie potencjału pracowników m.in. w zakresie śledzenia nieprawidłowości działania i występowania incydentów naruszenia bezpieczeństwa,
– zwiększenie motywacji do przestrzegania zasad bezpieczeństwa podczas korzystania z systemu.

Do korzyści w aspekcie finansowym należy:
– zmniejszenie kosztów związanych z usuwaniem skutków wystąpienia zagrożeń i naruszenia bezpieczeństwa SI m.in. poprzez zmniejszenie kosztów braku dostępności systemu, zmniejszenie kosztów napraw oraz zmniejszenie kosztów odzyskiwania danych.
– zmniejszenie kosztów szkoleń ze względu na wzrost świadomości użytkowników.

4. Charakterystyka dobrej praktyki

4.1. Założenia i funkcje dobrej praktyki

Dobra praktyka zakłada przeprowadzanie kontroli zabezpieczeń stanowisk i urządzeń komputerowych z wykorzystaniem metody list audytowych. Dane uzyskane podczas kontroli podlegają następnie analizie, co pozwala na wychwycenie słabości systemu i wdrożenie odpowiednich zabezpieczeń. Na najniższym poziomie dojrzałości kontroli podlegają tylko wybrane stanowiska i urządzenia komputerowe. Poziomy wyższe zakładają kontrolę zabezpieczeń wszystkich stanowisk i urządzeń oraz opracowanie sformalizowanej metody oceny poziomu bezpieczeństwa poszczególnych stanowisk komputerowych. Umożliwia to zarówno porównywanie poziomu bezpieczeństwa stanowisk, jak i monitorowanie tego poziomu w zmieniających się warunkach.

Dobra praktyka należy do grupy zabezpieczeń organizacyjnych (Madej 2010), a podstawowe spełniane przez nią funkcje to:
– wykrywanie braków, błędów i nieprawidłowości w zabezpieczeniach,
– monitorowanie sytuacji w zakresie zabezpieczeń systemu informatycznego,
– uświadamianie użytkowników w zakresie funkcjonowania zabezpieczeń.

Pośrednio spełnia ona także takie funkcje, jak: zapobieganie, ograniczanie i poprawianie (m.in. poprzez wykrywanie błędów, braków i nieprawidłowości w zabezpieczeniach, co pozwala je następnie usunąć i zapobiec skutkom ich

wystąpienia) oraz odstraszanie (w sytuacji gdy świadomość przeprowadzania kontroli powstrzymuje użytkowników przed próbami nadużyć).

4.2. Tworzenie list audytowych

Lista audytowa ma postać zbioru pytań, na które użytkownik odpowiada, najczęściej w sposób binarny: „tak"/„nie", („jest"/„nie ma"; „spełnione"/„niespełnione") z zachowaniem możliwości udzielenia odpowiedzi „nie dotyczy" lub „nie wiem". Czasami dopuszcza się odpowiedź: „spełnione częściowo". Listy pozwalają na zbieranie informacji o systemie oraz dokonanie jego wzorcowej oceny, dlatego są wykorzystywane do kontroli zabezpieczeń oraz do określenia poziomu bezpieczeństwa całego systemu lub jego fragmentów.

Gdy są odpowiednio skonstruowane, ich wykorzystanie nie sprawia dużych problemów. Po udzieleniu odpowiedzi na wszystkie pytania widać, których elementów nie ma w systemie. Ich zaletą jest natychmiastowe zwrócenie uwagi na występujące problemy, elementy systemu i zjawiska, które mają znaczenie dla bezpieczeństwa systemu. To z kolei powinno być punktem wyjścia do podjęcia dalszych działań.

Wykorzystanie list do określania poziomu bezpieczeństwa systemu polega na odpowiednim skonstruowaniu wzorca, który określa stan idealny i maksymalną liczbę punktów, jaką może uzyskać kontrolowany system. Wzorzec stanowi więc odniesienie dla uzyskanych wyników. Następnie do poszczególnych pytań przypisuje się liczbę punktów za odpowiedź pozytywną i negatywną (najczęściej 1 za „tak"/„jest"/„spełnione" i 0 za „nie"/„nie ma"/„niespełnione"). Po udzieleniu odpowiedzi na wszystkie pytania, punkty należy zsumować i wynik porównać ze wzorcem.

Pytania zawarte w listach muszą być szczegółowe i jednoznaczne, tak aby odpowiadający nie miał żadnych wątpliwości, jakiej udzielić odpowiedzi. W przypadku wykorzystywania list do określenia poziomu bezpieczeństwa istotne jest również, żeby waga poszczególnych pytań była zbliżona, a jeżeli nie jest, to należy dokonać korekty np. poprzez przypisanie im różnej liczby punktów. W celu ułatwienia analizy uzyskanych wyników pytania mogą być podzielone na różne kategorie (np. dotyczące tego samego fragmentu systemu). Żeby opracowana lista audytowa była użyteczna, musi spełniać kilka warunków:

– nie może pomijać żadnego istotnego elementu – zestaw pytań musi obejmować cały badany obszar (system lub jego fragment),

– w przypadku elementów o różnym poziomie istotności należy przypisać pytaniom odpowiednie wagi, dać różną liczbę punktów za odpowiedź lub zadać różną liczbę pytań na ich temat (jest to szczególnie ważne przy wykorzystywaniu list do określania poziomu bezpieczeństwa),

– należy ustalić wzorce (np. klasy bezpieczeństwa systemu) i odpowiadające im progi punktowe,

– odpowiedzi muszą być udzielone zgodnie ze stanem faktycznym.

Należy zaznaczyć, że przy wykorzystywaniu list do określania poziomu bezpieczeństwa nawet spełnienie wszystkich wymienionych warunków pozwala uzyskać wynik, który tylko wskazuje, o ile stan faktyczny odbiega od stanu wzorcowego, a nieodpowiednia konstrukcja wzorca nie będzie dawała wiarygodnych wyników.

W przypadku omawianej dobrej praktyki listy audytowe muszą być dostosowane do poszczególnych rodzajów stanowisk i urządzeń komputerowych, które będą podlegać kontroli. W ich opracowaniu powinny uczestniczyć służby informatyczne i osoba pełniąca funkcję administratora bezpieczeństwa informacji. Jako podstawę do opracowania list kontrolnych należy przyjąć m.in.:

– normy PN-ISO/IEC 27001 i PN-ISO/IEC 17799:2007 (odpowiednik normy ISO/IEC 27002),

– akty prawne dotyczące wymogów w zakresie zarządzania bezpieczeństwem informacji,

– ustawę o ochronie danych osobowych wraz z rozporządzeniami,

– dokumenty wewnętrzne dotyczące zarządzania bezpieczeństwem informacji,

– własne doświadczenia oddziału informatyki i ABI,

– gotowe wzorce list audytowych.

Pytania na liście powinny być podzielone na określone obszary (kategorie), które mają wpływ na bezpieczeństwo, i w tych obszarach powinno się zadawać pytania dotyczące zabezpieczeń. Przykładowe obszary i zawarte w nich pytania mogą przedstawiać się następująco (poniższe obszary wyróżniono zgodnie z normą PN-ISO/IEC 17799:2007):

– opracowanie polityki bezpieczeństwa, np. czy pracownik zna dokument polityki bezpieczeństwa?

– organizacja bezpieczeństwa, np. czy stanowisko zabezpieczone jest przed dostępem osób trzecich?

– klasyfikacja i kontrola aktywów, np. czy zasoby na stanowisku komputerowym są zinwentaryzowane?

– bezpieczeństwo osobowe, np. czy pracownik brał udział w szkoleniach z zakresu bezpieczeństwa?

– bezpieczeństwo fizyczne i środowiskowe, np. czy stanowisko komputerowe jest zabezpieczone przed utratą zasilania?

– zarządzanie systemami i sieciami, np. czy wszystkie zużyte nośniki danych są niszczone?

– kontrola dostępu do systemu, np. czy pracownik nie zostawia włączonego komputera, gdy wychodzi z pomieszczenia?

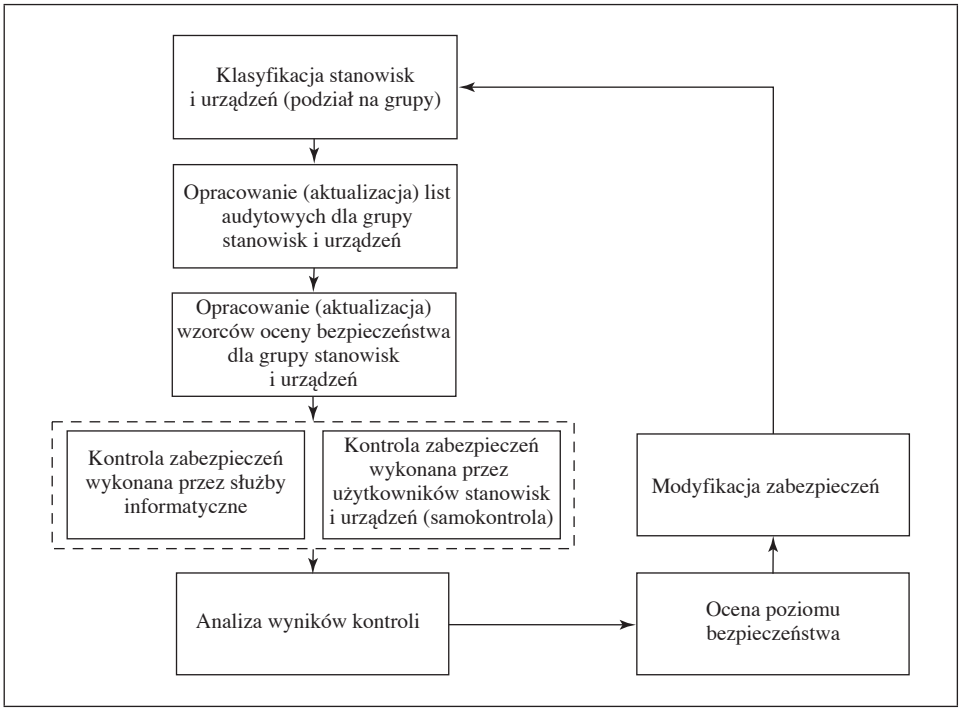
– rozwój i utrzymywanie systemu, np. czy do podpisania dokumentów elektronicznych pracownik wykorzystuje podpis cyfrowy?

– zarządzanie ciągłością działania, np. czy dla stanowiska komputerowego zdefiniowane są procedury postępowania na wypadek awarii?

– zgodność z przepisami prawa i specyfikacją techniczną, np. czy pracownik zna wymogi prawne dotyczące przetwarzania danych osobowych na stanowisku komputerowym?

Przytoczone pytania mają charakter przykładowy, powinny być dostosowane do potrzeb.

Docelowe etapy realizacji dobrej praktyki (na najwyższym poziomie dojrzałości) przedstawione zostały na rys. 2.



Rys. 2. Etapy realizacji dobrej praktyki w zakresie kontroli zabezpieczeń stanowisk i urządzeń komputerowych

Źródło: opracowanie własne.

Należy zaznaczyć, że w celu ułatwienia zbierania wyników, ich analizy i oceny do przeprowadzania kontroli niezbędne jest narzędzie informatyczne wspomagające ten proces, np. formularz internetowy z możliwością zapisywania wyników w bazie.

4.3. Poziomy dojrzałości dobrej praktyki

Poziom I – kontrola zabezpieczeń wybranych stanowisk i urządzeń komputerowych. Na tym poziomie dojrzałości kontrola zabezpieczeń powinna być przeprowadzona w odniesieniu do wybranych stanowisk i urządzeń komputerowych. Wybór stanowisk powinien być uzależniony m.in. od:

– znaczenia i rodzaju informacji przetwarzanych na stanowisku (urządzeniu) komputerowym,

– zagrożeń, na jakie narażone jest stanowisko (urządzenie),

– podatności na zagrożenia, jakimi charakteryzuje się stanowisko (urządzenie).

Realizacja dobrej praktyki na tym poziomie składa się z następujących po sobie etapów, takich jak:

– wybór stanowisk i urządzeń komputerowych,

– klasyfikacja stanowisk i urządzeń (podział na grupy),

– opracowanie list audytowych dla danych grup stanowisk lub urządzeń,

– przeprowadzenie kontroli zabezpieczeń przez pracowników oddziału informatyki oraz przez użytkowników stanowisk i urządzeń,

– analiza wyników kontroli pod kątem poprawności działania zabezpieczeń,

– modyfikacja zabezpieczeń,

– aktualizacja list audytowych.

Etap „modyfikacja zabezpieczeń" jest reakcją na wykryte podczas analizy braki i nieprawidłowości w funkcjonowaniu zabezpieczeń, a „aktualizacja list audytowych" wynika z wniosków wyciągniętych podczas analizy oraz konieczności uwzględniania takich czynników, jak: upływ czasu, zmiany w systemie czy pojawianie się nowych zagrożeń.

Poziom II – kontrola zabezpieczeń wszystkich stanowisk i urządzeń komputerowych. Poziom ten funkcjonalnie nie różni się od poziomu pierwszego. Różnica polega na tym, że kontrola zabezpieczeń dotyczy wszystkich stanowisk i urządzeń komputerowych, w tym także służbowych urządzeń mobilnych, takich jak: laptopy, tablety czy smartfony. Na tym poziomie konieczne jest sklasyfikowanie wszystkich urządzeń i opracowanie dla nich odpowiednich rodzajów list audytowych uwzględniających ich specyfikę i sposób użytkowania. Szczególnie istotne jest kontrolowanie urządzeń, które są użytkowane poza siedzibą sądu.

Poziom III – ocena poziomu bezpieczeństwa stanowisk i urządzeń komputerowych. Na tym poziomie dodatkowym elementem jest zaimplementowanie wzorcowej oceny poziomu bezpieczeństwa stanowisk komputerowych. Wymaga to stworzenia odpowiedniego wzorca oceny dla każdego rodzaju stanowiska i urządzenia komputerowego. Na tym poziomie kolejno następują po sobie etapy:

– klasyfikacja stanowisk i urządzeń (podział na grupy),

– opracowanie list audytowych dla danych grup stanowisk lub urządzeń,

– opracowanie wzorców oceny poziomu bezpieczeństwa dla danych rodzajów stanowisk i urządzeń (etap dodatkowy),

– przeprowadzenie kontroli zabezpieczeń przez pracowników oddziału informatyki oraz przez użytkowników stanowisk i urządzeń,

– analiza wyników kontroli pod kątem poprawności działania zabezpieczeń,

– ocena poziomu bezpieczeństwa (etap dodatkowy),

– modyfikacja zabezpieczeń,

– aktualizacja list audytowych,

– aktualizacja wzorców oceny (etap dodatkowy).

Etap „aktualizacja wzorców oceny" wynika, podobnie jak „aktualizacja list audytowych", z wniosków wyciągniętych podczas analizy oraz konieczności uwzględniania takich czynników, jak: upływ czasu, zmiany w systemie czy pojawianie się nowych zagrożeń.

4.4. Koszty wdrożenia dobrej praktyki

Na koszt wdrożenia dobrej praktyki składa się:

– koszt opracowania i późniejszej aktualizacji list audytowych oraz wzorca oceny poziomu bezpieczeństwa,

– koszt analizy wyników kontroli i oceny poziomu bezpieczeństwa,

– koszt opracowania informatycznych narzędzi wspomagających przeprowadzanie kontroli, analizowanie wyników i ocenianie poziomu bezpieczeństwa,

– koszt przeszkolenia osób odpowiedzialnych za funkcjonowanie praktyki,

– koszt przeprowadzania kontroli zabezpieczeń stanowisk i urządzeń komputerowych przez pracowników działu informatyki oraz przez użytkowników stanowisk i urządzeń.

Wymienione koszty są przede wszystkim kosztami pracy służb informatycznych (głównie na opracowanie list audytowych, narzędzi wspomagających i przeprowadzanie kontroli) oraz kosztami pracy użytkowników poniesionymi na samokontrolę swoich stanowisk i urządzeń.

5. Wnioski z wdrożenia dobrej praktyki

Dobra praktyka z zakresu kontroli zabezpieczeń stanowisk i urządzeń komputerowych została wdrożona w 17 sądach: w 13 w ramach pilotażu podstawowego i w 4 sądach w ramach pilotażu uzupełniającego (*Badanie ewaluacyjne…* 2015). Wśród sądów, które wybrały dobrą praktykę, był m.in. Sąd Apelacyjny w Białymstoku, Sąd Okręgowy w Rzeszowie, Sąd Rejonowy dla Krakowa-Nowej Huty

w Krakowie, Sąd Rejonowy w Mikołowie, Sąd Rejonowy w Gliwicach, Sąd Rejonowy w Chorzowie.

Harmonogram wdrażania oraz poziom zaawansowania prac w poszczególnych sądach pilotażowych zamieszczone zostały w opracowaniu (*Raport całościowy…* 2014).

Z opublikowanych raportów i informacji uzyskanych podczas współpracy autora z firmą wdrażającą można wyciągnąć kilka końcowych wniosków. Wdrażanie praktyki miało bardzo pozytywny wpływ na ogólne zagadnienie bezpieczeństwa systemów informatycznych w sądach, które ją wybrały. Podczas jej wdrażania w poszczególnych sądach przeprowadzone zostały dodatkowe prace i usprawnienia, których praktyka bezpośrednio nie obejmowała, a których wykonanie przy okazji jej wdrażania stało się o wiele prostsze. Do prac tych zaliczyć należy:

– weryfikację polityki bezpieczeństwa sądu,

– sprawdzenie systemu informatycznego sądu pod kątem spełniania wymogów Krajowych Ram Interoperacyjności (KRI),

– opracowanie procedur okresowej kontroli bezpieczeństwa informatycznego stanowisk pracy,

– przeprowadzenie kompleksowego audytu stanowisk i urządzeń komputerowych,

– zapewnienie wsparcia w zakresie bezpieczeństwa wybranych stanowisk komputerowych,

– przeprowadzenie warsztatów i szkoleń z zakresu bezpieczeństwa informatycznego,

– opracowanie rekomendacji przygotowujących do przeprowadzenia audytu informacji przez audytora zewnętrznego.

Po zakończonym wdrożeniu, na podstawie przeprowadzonych wywiadów z pracownikami sądów (metodą ITI i CAWI), wskazano najważniejsze zalety i ograniczenia dobrej praktyki oraz oceniono jej efekty. Do głównych jej zalet należy:

– wdrożenie audytu stanowisk pracy,

– zweryfikowanie na podstawie anonimowej ankiety poziomu wiedzy pracowników sądu na temat polityki bezpieczeństwa i ochrony danych osobowych,

– podniesienie poziomu bezpieczeństwa infrastruktury informatycznej,

– ustalenie słabych obszarów w zakresie audytu stanowisk komputerowych,

– wdrożenie modułu e-learningu z treściami obejmującymi problematykę bezpieczeństwa informatycznego.

Do jej ograniczeń i trudności podczas wdrażania zaliczono:

– dodatkowe zadania (obciążenie) pracowników sądu wynikające z realizacji praktyki,

– możliwe przekłamanie podczas wypełniania ankiet i list kontrolnych wynikające z braku wiedzy pracowników sądu,

– konieczność odpowiedniego przeszkolenia pracowników w celu osiągnięcia prawidłowych wyników.

Ostatecznie za najważniejsze efekty, które przyniosło wdrożenie dobrej praktyki, pracownicy sądów uznali:

– wychwycenie słabych stron działania systemów informatycznych i opracowanie adekwatnych rozwiązań eliminujących zagrożenia bezpieczeństwa SI,

– zwiększenie świadomości pracowników sądów na temat zagrożeń związanych z nieprzestrzeganiem zasad bezpieczeństwa podczas użytkowania stanowisk i urządzeń komputerowych,

– wprowadzenie systematycznych kontroli celem monitorowania istniejących zabezpieczeń oraz wychwytywania nowych zagrożeń i szybkiego na nie reagowania.

Należy także wspomnieć, że opracowywanie koncepcji dobrych praktyk i współpraca ze środowiskiem sądowym były interesującym doświadczeniem, dlatego obecnie zespół realizujący projekt przygotowuje badania, które pozwolą ocenić efekty wdrożenia dobrych praktyk informatycznych.

Literatura

Badanie ewaluacyjne pilotażu wdrażania dobrego zarządzania jednostkami wymiaru sprawiedliwości w ramach projektu „PWP Edukacja w dziedzinie zarządzania czasem i kosztami postępowań sądowych – case management". Raport końcowy (2015), ASM – Centrum Badań i Analiz Rynku, Kutno.

Baskerville R.L. (1999), *Investigating Information Systems with Action Research, Communications of the Association for Information Systems*, vol. 2, Article 19, http://aisel.aisnet.org/cais/vol2/iss1/19 (data dostępu: 15.09.2014).

Baskerville R.L., Wood-Harper A.T. (1996), *A Critical Perspective on Action Research as a Method for Information Systems Research*, „Journal of Information Technology", vol. 11, nr 3, https://doi.org/10.1080/026839696345289.

COBIT 4.1. Metodyka. Cele kontrolne. Wytyczne zarządzenia. Modele dojrzałości (2010), IT Governance Institute, Stowarzyszenie Audytu, Bezpieczeństwa i Kontroli Systemów Informacyjnych ISACA, Warszawa.

Cole M., Avison D. (2007), *The Potential of Hermeneutics in Information Systems Research*, „European Journal of Information Systems", vol. 16, nr 6, https://doi.org/10.1057/palgrave.ejis.3000725.

Davis C., Schiller M., Wheeler K. (2011), *IT Auditing Using Controls to Protect Information Assets*, McGraw-Hill, New York.

Davison R.M., Martinsons M.G., Kock N. (2004), Principles of Canonical Action Research, „Information Systems Journal", vol. 14, nr 1, https://doi.org/10.1111/j.1365-2575.2004.00162.x.

Grabowski M., Madej J., Trąbka J. (2018), *Koncepcja metodyki projektowania i wdrażania dobrych praktyk informatycznych dla sądów powszechnych*, „Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie", nr 4(976), https://doi.org/10.15678/ZNUEK.2018.0976.0413.

Informatyzacja postępowania cywilnego. Teoria i praktyka (2016), red. K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek, Seria Monografie Prawnicze, C.H. Beck, Warszawa.

Landoll D. (2011), *The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments*, CRC Press, Boca Raton, FL, USA.

Liderman K. (2008), *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Wydawnictwo Naukowe PWN SA, Warszawa.

Liderman K., Patkowski A. (2003), *Metodyka przeprowadzania audytu z zakresu bezpieczeństwa teleinformatycznego*, „Biuletyn Instytutu Automatyki i Robotyki", nr 19.

Madej J. (2009), *Prawne wymogi bezpieczeństwa systemów informatycznych w polskich przedsiębiorstwach*, „Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie", nr 770.

Madej J. (2010), *Klasyfikacja zagrożeń bezpieczeństwa systemu informatycznego*, „Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie", nr 814.

Molski M., Łacheta M. (2006), *Przewodnik audytora systemów informatycznych*, Helion, Gliwice.

Paulk M.C., Weber C.V., Curtis B., Chrissis M.B. (1993), *Capability Maturity Model for Software* (*Version 1.1*), Technical Report CMU/SEI-93-TR-024 ESC-TR-93-177, February, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, https://resources.sei.cmu.edu/asset_files/TechnicalReport/1993_005_001_16211.pdf, (data dostępu: 13.04.2018).

Polaczek T. (2006), *Audyt bezpieczeństwa informacji w praktyce*, Helion, Gliwice.

Polska Norma PN-I-13335-1:1999. Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Pojęcia i modele bezpieczeństwa systemów informatycznych (1999), Polski Komitet Normalizacyjny, Warszawa.

Polska Norma PN-ISO/IEC 17799:2007. Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem informacji (2007), Polski Komitet Normalizacyjny, Warszawa.

Quinn S.D., Souppaya M., Cook M., Scarfone K. (2018), *National Checklist Program for IT Products – Guidelines for Checklist Users and Developers*, National Institute of Standards and Technology, https://doi.org/10.6028/NIST.SP.800-70r4.

Raport całościowy z wdrożenia za okres od 1 grudnia 2013 r. do 24 października 2014 r. (2014), oprac. WYG International, WYG Consulting, WYG PSDB, Uniwersytet Ekonomiczny w Krakowie, Instytut Allerhanda na zlecenie Krajowej Szkoły Sądownictwa i Prokuratury, http://www.efs2007-2013.gov.pl/Dokumenty (data dostępu: grudzień 2016).

Common Courts and IT Good Practice in the Security Auditing of Workstations and Computers Devices

(Abstract)

The article presents the concept of IT good practice on security controls for workstations and computing devices using checklists. The concept of good practice was formulated during implementation of the project "Education in time management and cost management of judicial proceedings – case management" (a part of the Human Capital Programme). This project was one of the components supporting the reform of the Polish judiciary and was aimed at increasing the efficiency of the judicial system by lowering costs and increasing the skills of those employed in the judiciary. The paper describes the use of checklists for security audits of computer systems at the level of computer workstations and computer equipment. It presents the conditions and background of this practice (legal acts, international security standards), the purpose and benefits of its implementation, and the basic assumptions, scope and functions that should be implemented at different maturity levels and the conclusions of the implementation of good practice.

Keywords: IT security, audit, checklists, IT good practices, judiciary, courts.