PRZEGLĄD TELEINFORMATYCZNY
NR 1-2, 2018

Zintegrowane badanie i ocena stanu ochrony zasobów informacji

Krzysztof LIDERMAN, Adam E. PATKOWSKI

Instytut Teleinformatyki i Automatyki, Wydział Cybernetyki WAT,
ul. Generała W. Urbanowicza 2, 00-908 Warszawa
krzysztof.liderman@wat.edu.pl, adam.patkowski@wat.edu.pl

STRESZCZENIE: W artykule przedstawiono propozycję zintegrowanego ujęcia zagadnień oceny stanu ochrony informacji w złożonych systemach informacyjnych. Fundamentem tej propozycji jest diagnostyka techniczna oraz bezpieczeństwo informacyjne. Przedstawiono m.in. zagadnienia wykonywania badań dostarczających podstaw do takiej oceny: testów penetracyjnych oraz audytu bezpieczeństwa teleinformatycznego. W ostatnim punkcie opisano krótko metodykę LP-A wykonywania audytu bezpieczeństwa teleinformatycznego integrującą różne typy badań oraz ułatwiającą wykorzystanie różnych, w zależności od potrzeb, wzorców audytowych.

SŁOWA KLUCZOWE: ochrona informacji, bezpieczeństwo informacyjne, diagnostyka, audyt, testy penetracyjne, metodyka LP-A

1. Wprowadzenie

Coraz większa złożoność „świata informacyjnego" sprawia, że osoby odpowiedzialne za szeroko rozumiane przetwarzanie informacji oraz właściciele tych informacji tracą do niego zaufanie i szukają sposobów upewnienia się, że ich informacje są „bezpieczne". To m.in. powoduje wzrost zleceń na wykonywanie „testów bezpieczeństwa" i „audytów bezpieczeństwa" mających, w rozumieniu zamawiających, dać obiektywną odpowiedź na temat „bezpieczeństwa informacji", czy też, ujmując problem nieco inaczej – obiektywną ocenę stanu zabezpieczeń informacji. Niestety, podstawowy kłopot polega na tym, że samo pojęcie „bezpieczeństwo" jest rozmyte, a słowa takie jak „testowanie" i „audyt" oznaczają pewne ściśle określone przedsięwzięcia, często znacznie odbiegające od ich popularnego (czytaj także: powierzchownego) rozumienia. Dodatkowo, z powodu łączenia sieci różnych typów (patrz np. [6], [7]), zagadnienia określenia

stanu ochrony informacji przesuwają się z obszaru prostych systemów komputerowych do obszaru złożonych urządzeń i systemów (elektromechanicznych, elektronicznych, itp.) w których „element przetwarzania informacji" jest tylko jednym z wielu elementów składających się na takie urządzenia lub systemy.

W niniejszym artykule przedstawiono propozycję zintegrowanego ujęcia zagadnień oceny stanu ochrony informacji w złożonych systemach informacyjnych. Fundamentem tej propozycji jest *diagnostyka techniczna* (patrz punkt 2) oraz perspektywa *bezpieczeństwa informacyjnego*, gdzie bezpieczeństwo informacji jest jego warunkiem koniecznym.

DEFINICJA 1

Bezpieczeństwo informacyjne oznacza uzasadnione zaufanie podmiotu do jakości i dostępności pozyskiwanej oraz wykorzystywanej informacji.

• • • •

Definicja 1 implikuje wykorzystanie kryteriów jakości informacji – są nimi np. relewantność, spójność, dokładność, kompletność, wiarygodność, ale także *bezpieczeństwo*.

DEFINICJA 2

Bezpieczeństwo informacji oznacza uzasadnione zaufanie podmiotu, że nie zostaną poniesione straty wynikające z niepożądanej zmiany, na skutek realizacji zagrożenia, wymaganych wartości istotnych kryteriów jakości informacji.

• • • •

Wymienione w definicji 2 „uzasadnione zaufanie podmiotu" osiąga się zwykle poprzez wykonanie analizy ryzyka i przyjęcie odpowiednich metod postępowania z ryzykiem. Natomiast jakie kryteria jakości są „istotne" dla poszczególnych kategorii informacji oraz konkretnych uwarunkowań jej przetwarzania zwykle określają, w przypadku organizacji biznesowej w której takie informacje są przetwarzane i wykorzystywane, gremia kierownicze tej organizacji (podmiotu) przy pomocy odpowiednich służb. Zwykle kryteriami tymi będą tajność, integralność oraz dostępność informacji. Bardziej szczegółowa dyskusja zagadnień bezpieczeństwa informacyjnego jest zamieszczona w rozdziale 1 w [6].

Ocena to sąd wartościujący, wszelka wypowiedź wyrażająca pozytywne lub negatywne ustosunkowanie się wypowiadającego do kogoś lub czegoś. W dziedzinie techniki, w szczególności w dziedzinie bezpieczeństwa informacyjnego, zasadniczą czynnością procesu oceny jest zbieranie danych stanowiących podstawę opracowania wskaźników, na podstawie których będą wydawane sądy np. o stopniu osiągnięcia założonych celów stawianych przed

zabezpieczeniami. Oceniający ma się zatem wypowiedzieć na temat skuteczności i poprawności spełniania funkcji zabezpieczenia przez obiekt oceniany (czyli potocznie – jakości zabezpieczeń). Ten proces wypracowywania oceny i samą ocenę zwykle nazywa się (niepoprawnie – patrz np. rozdz.5 w [5]) *pomiarem bezpieczeństwa*.

Na przestrzeni ostatnich kilkunastu lat nastąpiło, pod wpływem m.in. upowszechnienia technologii komunikacyjnych i informatycznych, zwyrodnienie (bo tak to chyba trzeba nazwać) pojęć i przedsięwzięć związanych z określaniem cech jakościowych różnych obiektów, w tym takiego szczególnego obiektu jak informacja. Wystarczy zajrzeć do będącej w dzisiejszych czasach wyrocznią Wikipedii (polskojęzycznej) żeby stwierdzić, że w dziedzinie techniki *test* i *testowanie* dotyczy tylko oprogramowania – nie bierze się pod uwagę, że są jeszcze inne elementy systemu informacyjnego, które mogą mieć wpływ na jakość (w tym bezpieczeństwo) związanych z nim zasobów informacji, zaś związki pomiędzy takimi pojęciami i przedsięwzięciami jak *diagnozowanie* i *testowanie* nie istnieją (przynajmniej na poziomie haseł Wikipedii).

2. Diagnostyka techniczna

Dla urządzeń złożonych, jakimi są współczesne systemy cyfrowe, proste metody badań diagnostycznych są często niewystarczające. Dąży się więc do stworzenia i wprowadzenia dokładniejszych metod badania systemów (także w celu automatyzacji procesu ich obsługi) wykorzystujących określony aparat formalny. Jest to obszar dziedziny nauki i techniki nazywany diagnostyką techniczną czy też, w nowszych publikacjach (np. [12]), diagnostyką systemową. *Diagnostyka techniczna* [11] to dziedzina nauki i techniki, zajmująca się opracowaniem oraz wykorzystaniem (czyli teorią i zastosowaniem) metod i środków służących badaniu stanu technicznego systemów. W tym artykule przedmiotem rozważań są złożone systemy cyfrowe (jako podklasa systemów technicznych) i ich dotyczą przedstawione dalej definicje i uwagi.

Badania, na podstawie których jest formułowana diagnoza badanego obiektu, polegają na wykonaniu określonego zestawu sprawdzeń [11]. *Sprawdzeniem* nazywa się ciąg operacji badania wybranej cechy obiektu diagnozowanego, polegających na skontrolowaniu jej wartości i porównaniu z wzorcem. Podstawowymi czynnościami każdego sprawdzenia są:

- pobudzenie tej części obiektu, od której zależy wartość sprawdzanej cechy;
- odczytanie uzyskanej odpowiedzi (sygnału diagnostycznego);
- porównanie wartości odczytanej z przedziałem wartości dopuszczalnych.

W szczególnym przypadku sprawdzenie może obejmować pojedynczy element (podzespół) obiektu i sprawdzenie takie jest nazywane sprawdzeniem cząstkowym. Częściej jednak sprawdzeniu podlega kilka bądź kilkanaście elementów i w takim przypadku mówi się o torze sprawdzenia. *Torem sprawdzenia* nazywa się podzbiór tych elementów systemu, których stan ma wpływ na wartość badanej cechy diagnostycznej. Proces diagnozowania można zatem zdefiniować następująco:

DEFINICJA 3

Proces diagnozowania to ciąg operacji polegających na wykonaniu określonego zestawu sprawdzeń i analizowaniu uzyskanych wyników w celu rozpoznania stanu, jaki ma miejsce w chwili t_0 zakończenia badania.

• • • •

Diagnozą nazywa się wypowiedź przeprowadzającego badanie o stanie (np. bezpieczeństwa) badanego obiektu. Niech będą dane:

- R – relacje pomiędzy objawami (zestawami wyników sprawdzeń) charakterystycznymi dla poszczególnych stanów a stanami obiektu,
- D – zbiór wyników sprawdzeń (objawów),
- $D_l(t_0)$ – zbiór objawów uzyskany w chwili diagnozowania t_0,
- E – zbiór stanów obiektu,
- $\Delta E_l(t_0)$ – diagnoza o stanie E_l dla chwili t_0.

Można sformułować następującą, tzw. *podstawową regułę diagnostyki* [11]:

DEFINICJA 4

Jeżeli jest znana relacja R, oraz uzyskano w procesie diagnozowania konkretny zbiór objawów D_l, to można sformułować diagnozę ΔE_l o stanie obiektu w chwili badania t_0.

• • • •

Regułę tę symbolicznie można zapisać następująco:

$$R(D_1, E_1) \wedge D_l(t_0) \Rightarrow \Delta E_l(t_0)$$

Czytelnicy obeznani z systemami eksperckimi zapewne zauważą, że reguła ta, w kategoriach terminologicznych systemów eksperckich, jest tzw. *regułą produkcji*.

Warto zwrócić uwagę, że diagnoza sformułowana dla pewnej chwili t_0 jest prawdziwa tylko dla tej chwili t_0. Ma to odzwierciedlenie w raportach z badań technicznych, głównie testów penetracyjnych – podaje się czasy wykonywania badań oraz aktualność wykorzystywanych baz (eksploitów, poprawek, informacji o podatnościach itp.).

3. Testowanie jako element diagnostyki technicznej

Wprowadzony w poprzednim punkcie termin „sprawdzenie", używany w diagnostyce technicznej, jest odpowiednikiem używanego w informatyce terminu „test". W tym artykule rozważane są takie obiekty techniczne jak systemy informacyjne oraz będące elementami takich systemów obiekty cyfrowe. Mając to na uwadze, podstawowe typy badań wykonywanych w procesie zapewniania jakości (w tym bezpieczeństwa) takich obiektów można wyspecyfikować jako badanie:

1. *Elementów konstrukcyjnych*/*modułów* – jest to badanie elementów konstrukcyjnych (w przypadku oprogramowania – programu lub modułów wykonywalnych) w celu sprawdzenia, czy nie zawierają one błędów powstałych podczas analizy, projektowania lub wytwarzania. Ponieważ nie wszystkie moduły da się przetestować korzystając z tzw. pilotów (modułów sterujących przebiegiem testowania) i namiastek (nazywanych też makietami lub zaślepkami) – ich testowanie trzeba wtedy odłożyć do etapu scalania systemu.
2. *Scalania* (ang. *integration test*) – jest to badanie polegające na stopniowym konstruowaniu systemu i wykrywaniu błędów związanych z niepożądanymi zależnościami pomiędzy poszczególnymi elementami konstrukcyjnymi (w przypadku oprogramowania – modułami). Celem jest zbudowanie z oddzielnych, przetestowanych elementów, systemu działającego zgodnie z projektem jego architektury. Scalanie może dotyczyć:
   – modułów w system programowy;
   – oprogramowania ze sprzętem (np. w systemach sterowania).
3. *Zgodności* (ang. *compliance test*) – jest to badanie systemu wykonywane w celu sprawdzenia, czy spełnia on określone wymagania, np. narzucone przez regulacje i standardy państwowe. Pomyślne przejście takich testów może być podstawą do wydania certyfikatu dla systemu.
4. *Systemu* – jest to badanie wykonywane w celu sprawdzenia, czy skonstruowany system spełnia wymagania określone przez użytkowników. Jest to szczególny przypadek badania zgodności.
5. *Odbiorcze* (ang. *acceptance test*) – jest to badanie systemu lub jego elementu, wykonywane zwykle przez zleceniodawcę (tj. podmiot, który zlecił skonstruowanie tego systemu i jest stroną umowy z wykonawcą), na jego żądanie, po zainstalowaniu w środowisku docelowym, z udziałem wykonawcy w celu sprawdzenia czy są spełnione wymagania zawarte w umowie.
6. *Weryfikacyjne* (ang. *verification test*) – jest to badanie wykonywane w celu sprawdzenia czy proces w cyklu rozwojowym systemu spełnia określone

wymagania w danym momencie (etapie) jego opracowywania, tj. czy metody i narzędzia są poprawnie dobrane i stosowane.

Badanie systemu, czyli wytworzonego, złożonego produktu jako całości, wymaga przeprowadzenia pewnych specjalnych testowań, takich jak:

1. *Testowanie wznowień* – polega na powodowaniu lub symulowaniu różnych awarii i sprawdzaniu zdolności systemu do dalszego działania (pożądany jest tzw. stopniowy „upadek" systemu [14]).
2. *Testowanie obciążeniowe* – polega na takim obciążeniu systemu, które spowoduje maksymalne zaangażowanie zasobów systemowych.
3. *Testowanie wrażliwości* – polega na badaniu różnych kombinacji danych wejściowych w celu wykrycia takich, które mogą spowodować niestabilność systemu lub błędy w przetwarzaniu danych lub działaniu.
4. *Testowanie efektywności* – polega na badaniu parametrów operacyjnych (np. czasu odpowiedzi) przy różnych obciążeniach.
5. *Testowanie regresyjne* to powtórne wykonanie niektórych testów w celu upewnienia się, że nowo wprowadzone zmiany nie wywołały niepożądanych skutków ubocznych. Testowanie regresyjne ma szczególne znaczenie na etapie:
   – scalania systemu,
   – eksploatacji (po wykonaniu czynności związanych z tzw. pielęgnacją systemu, np. po zainstalowaniu poprawek lub dołączeniu nowych elementów elektronicznych).

W przypadku testowania systemów sterowania pojawiają się kolejne elementy do przetestowania:

– dotrzymanie wymaganych zależności czasowych w różnych warunkach,
– współdziałanie sprzętu i oprogramowania.

Testowania wznowień, obciążeniowe, wrażliwości i efektywności są elementami składowymi ogólniejszego *testowania bezpieczeństwa,* które, z grubsza rzecz biorąc, polega na przeprowadzaniu badań systemu pod kątem możliwości nieuprawnionego dostępu do informacji, nieuprawnionej ingerencji w informację oraz możliwości jej uniedostępnienia. Badania takie są zwykle przeprowadzane w ramach audytów, których częścią powinny być wymienione wcześniej badania i testy oraz tzw. *testy penetracyjne* [10] i, w szczególnych przypadkach, badania podatności kodu programu na niepożądane manipulacje.

Testowanie stosuje się w celu wykrycia błędów w testowanym obiekcie. Aby test wykrył błąd, muszą wystąpić trzy elementy:

1. Musi nastąpić *dotarcie do błędu*. Dane wejściowe testu oraz stan testowanego obiektu muszą spowodować uaktywnienie tej części obiektu (np. wykonanie segmentu kodu) w której znajduje się błąd.

2. Musi nastąpić *uwolnienie awarii*. Błąd nie zawsze powoduje złe wyniki, pomimo że element z błędem (obwód elektroniczny, segment kodu, itp.) został uaktywniony. Wejście testu oraz stan testowanego obiektu muszą spowodować, że część obiektu w której tkwi błąd, wyprodukuje błędny wynik.
3. Awaria musi się *ujawnić*. Błędny wynik musi stać się widoczny dla osoby testującej lub automatycznego komparatora.

Użyte terminy „awaria" i „błąd" można zdefiniować następująco[1]:

– awaria – jest tak nazywana widoczna niezdolność obiektu testowanego lub jego elementu do wykonania wymaganej funkcji w określonych limitach. Awaria objawia się w postaci niepoprawnego wyjścia (wartości wyjściowych, które nie spełniają wymagań lub specyfikacji), zatrzymania awaryjnego lub niespełnienia wymagań dotyczących określonych nieprzekraczalnych terminów, np. przetwarzania czy przesyłania informacji.
– błąd (ang. *bug*) – jest tak nazywana nieoczekiwana i niezamierzona właściwość programu lub sprzętu, zwłaszcza taka, która powoduje jego wadliwe działanie. Błąd wykryty na etapie eksploatacji obiektu zwykle nazywa się *usterką*. Jako synonimy używa się też terminów: *omyłka* oraz *wada*.

Aby stwierdzić, czy obiekt przeszedł pomyślnie test, potrzebna jest tzw. *wyrocznia testowa*. Jest to mechanizm określania (może nim być ekspert), czy rzeczywiste wyniki testu zasługują na akceptację czy odrzucenie. Formalnie rzecz biorąc, potrzebny jest do tego *generator wyników* który będzie generował wyniki oczekiwane i *komparator*, który będzie porównywał wyniki rzeczywiste z oczekiwanymi. Odrębnym, nie poruszanym w tym artykule zagadnieniem, ale ściśle związanym z testowaniem, jest *zarządzanie błędami* [3].

W tzw. systemach krytycznych ze względu na bezpieczeństwo (ang. *safety-critical systems*) stosowane jest specjalne podejście – w cykl życia systemu wbudowuje się przedsięwzięcia mające na celu uzyskanie odpowiedniego poziomu bezpieczeństwa. Podstawowym przedsięwzięciem jest *analiza bezpieczeństwa* (patrz [14]). W ramach analizy bezpieczeństwa oceniana jest wartość ryzyka związanego z badanym lub projektowanym obiektem i identyfikowane są mechanizmy powstawania szkód w otoczeniu takiego obiektu, w szczególności występowania wypadków z udziałem ludzi. Zdarzenia prowadzące w sposób bezpośredni do wypadku nazywane są *hazardami,* które definiuje się jako sytuacje mogące spowodować śmierć lub obrażenia ludzi.

[1] W literaturze można spotkać także nieco się różniące objaśnienia podanych dalej terminów.

W projektowaniu systemów tej klasy należy uwzględnić specjalne wymagania, nie występujące przy „zwykłych" systemach informatycznych [13]. Do tych specjalnych wymagań, które powinny być zbadane (przetestowane) przed oddaniem systemu do eksploatacji, będą należały wymagania dotyczące:

- przejścia w „stan bezpieczny" w przypadku uszkodzeń i awarii (ang. *fail-safe*). Stan bezpieczny elementu badanego obiektu (systemu) to taki stan, w którym ten element nie stwarza zagrożeń dla obiektu i jego otoczenia, co często osiąga się poprzez ograniczenie funkcji lub dostępności obiektu (systemu),
- detekcji i obsługi błędów (sprzętowych i programowych),
- samotestowania (ang. *selftesting*),
- nadzoru sprzętowego lub programowego nad czasem realizacji funkcji (ang.*watchdog*),
- kontroli uprawnień w trakcie dostępu do zasobów.

Relację elementu obiektu w „stanie bezpiecznym" do pozostałej części obiektu opisują następujące zasady:

- element generuje specjalną sekwencję zdarzeń obserwowalnych (na zewnątrz tego elementu) która pozwala pozostałej części obiektu właściwie zinterpretować aktualny stan elementu;
- nie powstają żadne zdarzenia wewnętrzne, które wyprowadzą ten element ze stanu bezpiecznego – tylko specjalna sekwencja zdarzeń zewnętrznych (obserwowalnych), generowanych przez otoczenie „elementu w stanie bezpiecznym", może wyprowadzić ten element z tego stanu.

W odróżnieniu od testowania np. systemu programowego, testowanie systemu bezpieczeństwa jest przedsięwzięciem kompleksowym w tym sensie, że obejmuje:

- testowanie poprawności działania zabezpieczeń sprzętowych zintegrowanych z systemem teleinformatycznym,
- testowanie poprawności działania zabezpieczeń programowych zintegrowanych z systemem teleinformatycznym,
- testowanie poprawności integracji ww. zabezpieczeń za pomocą testów scalania i regresyjnych,
- testowanie poprawności działania środków ochrony technicznej i fizycznej,
- sprawdzenie poprawności wdrożenia ochronnych rozwiązań organizacyjnych,
- sprawdzenie odporności personelu na ataki socjotechniczne oraz sprawdzenie współdziałania ww. środków i personelu w celu ochrony informacji przetwarzanej, przechowywanej i przesyłanej w chronionym systemie. To

sprawdzenie jest wykonywane za pomocą *testów penetracyjnych* (patrz punkt 4),

– przeprowadzenie testów zgodności z wzorcem certyfikacyjnym w przypadku wymagania wystawienia certyfikatu bezpieczeństwa lub przeprowadzenie testów odbiorczych.

Zgodnie z ogólnie uznanymi zasadami, przygotowanie do testowania należy zacząć już podczas specyfikowania wymagań na system ochrony, sporządzając m.in. plan testów. Podstawowe informacje niezbędne do zaprojektowania planu testów to ustalenie, według jakiego standardu/normy ma być oceniany docelowy system (czyli jakie „wzorcowe" wymagania powinien spełniać) oraz określenie docelowego poziomu ochrony. Kompleksowe badania systemu bezpieczeństwa przeprowadza się zwykle w ramach audytu tego systemu (zwykle jako *audytu bezpieczeństwa teleinformatycznego*, patrz punkt 5).

4. Testy penetracyjne jako szczególny przypadek testowania

Testy penetracyjne to jeden ze sposobów zbierania informacji w ramach badania bezpieczeństwa systemów, głównie w celu znalezienia podatności. Cechy wyróżniające testy penetracyjne spośród innych rodzajów poszukiwania podatności to [10]:

– potwierdzanie zidentyfikowanych podatności przez precyzyjne wskazanie (często poparte pokazem) skutecznych ataków te podatności wykorzystujących;

– przewaga technik heurystycznych, opartych zwykle na osobistym doświadczeniu realizujących je ekspertów nad ogólnymi, standardowymi technikami „badawczymi" i co się z tym wiąże, na ukrywanie przez firmy i ekspertów tych sposobów, dających przewagę rynkową nad konkurencją.

Testem penetracyjnym nazywa się także analizę scenariuszy hipotetycznych „ataków", mającą na celu weryfikację hipotezy o podatności badanego obiektu (lub jego odpowiednika). Analiza taka jest stosowana w przypadkach, gdy rzeczywisty test (np. próba ataku DoS) nie powinien być wykonany.

Należy podkreślić, że test penetracyjny nie jest audytem bezpieczeństwa teleinformatycznego. Podobnie badanie zabezpieczeń teleinformatycznych wyłącznie za pomocą automatycznego skanera to nie jest test penetracyjny; nie jest nim też działaniem według wcześniej ustalonej listy kontrolnej (tzw. *checklisty*).

Test penetracyjny to badanie techniczne mające dostarczyć, o ile jest wykonywane w ramach audytu bezpieczeństwa teleinformatycznego (patrz punkt 5), tzw. *dowodów audytowych* do rozstrzygnięcia problemów wskazanych przez audytorów wiodących. Test penetracyjny da odpowiedź na konkretne, dobrze określone zapytania z zakresu ochrony zasobów informacyjnych; audyt powinien dać odpowiedź na pytanie o stan ochrony zasobów informacyjnych organizacji jako całości, w odniesieniu do ustalonego wzorca.

Celem testu penetracyjnego jest pozyskanie jak największej ilości informacji o testowanym obiekcie i, jeśli będzie to możliwe, również udowodnienie możliwości przełamania zabezpieczeń. Zatem pytanie, na jakie ma dać odpowiedź test penetracyjny to: „jaką informację jest w stanie zdobyć intruz (przy określonych warunkach)?" a nie „czy da się włamać do systemu?"

Wynik testu penetracyjnego jest silnie uzależniony od umiejętności i jakości pracy zespołu testującego i od czasu trwania testu. Testy penetracyjne nie gwarantują znalezienia wszystkich podatności, a ich wynik zależy od tzw. frontowych systemów zabezpieczających. Poza tym, czasami trzeba mieć po prostu szczęście i wykonać właściwy test we właściwym czasie.

Ponieważ testy penetracyjne często porównuje się z działaniami intruzów próbujących wykorzystać znane im podatności, warto wspomnieć o zasadniczej różnicy w warunkach działania pentestera i intruza – czas trwania testów penetracyjnych jest ograniczony warunkami umowy pomiędzy zespołem pentesterów a zleceniodawcą, intruz takich ograniczeń nie ma.

Podstawowym opracowaniem wytyczającym trendy w badaniach metodą testów penetracyjnych jest OSSTMM (Open Source Security Testing Methodology Manual). OSSTM jest oficjalną metodyką ISECOM (Institute for Security and Open Methodologies) z zakresu wykonywania testów bezpieczeństwa, udostępnioną na licencji Creative Commons 3.0 Attribution.

Opracowania wspomagające wykonywanie testów penetracyjnych znaleźć można także na stronie fundacji OWASP – Open Web Application Security Project (*http://www.owasp.org*).

Wart polecenia jest także artykuł [10] wiążący metodykę LP-A (patrz dalej) z wykonywaniem testów penetracyjnych oraz opracowania [1] i [2] systematyzujące wykonywanie testów penetracyjnych aplikacji internetowych i prezentujące autorską metodykę PTER ich wykonywania. Szczególnie cenne są zamieszczone tam krótkie, rzeczowe prezentacje metodyk OSSTMM oraz OWASP.

5. Audyt jako szczególny przypadek badania jakości systemu ochrony informacji

Szczególnym rodzajem oceny jest *audyt*. Nazywa się tak postępowanie sprawdzające sposób i/lub wynik wykonania „czegoś" (budowy systemu zabezpieczeń, zarządzania informatyką, wydatkowania funduszy itp.) na zgodność z określonym wzorcem audytowym (wymaganiami lub standardami albo normami), wykonywane przez stronę niezależną.

Dobrym wzorcem dla audytu bezpieczeństwa jest standard: stanowi rodzaj *checklisty*, daje wektorową miarę „bezpieczeństwa", zapewnia, że nic co uznano za istotne nie zostanie pominięte, umożliwia powtarzalność badań. Wzorzec taki jednak słabo uwzględnia specyfikę badanego obiektu oraz nie daje pewności, że zabezpieczenia są szczelne, nie działają przeciw sobie oraz że badanie będzie dostatecznie wnikliwe. Gwoli ścisłości należy nadmienić, że polska Najwyższa Izba Kontroli nieco inaczej definiuje „wzorzec". Wzorcem według NIK [16] nie jest norma, standard czy specyfikacja wymagań, lecz jednostka sektora prywatnego lub publicznego (krajowa lub zagraniczna – szczegóły patrz rozdziale 5 w [6]).

Wspomniana wcześniej niezależność, w przypadku systemów informacyjnych (i w węższym znaczeniu, teleinformatycznych), musi być zachowana w stosunku do:

- zespołu projektującego lub budującego system informatyczny lub system zabezpieczeń;
- dostawców sprzętu i oprogramowania;
- organizacji podlegającej przeglądowi (w takim sensie, że w skład zespołu audytowego nie powinni wchodzić pracownicy organizacji zlecającej audyt).

Jeżeli ocena ma być rzetelna, to musi być oparta na obiektywnych przesłankach a nie subiektywnych odczuciach oceniającego. W przypadku audytu tymi obiektywnymi przesłankami są tzw. dowody audytowe. Za [16] dowody kontroli, zgodnie ze Standardami kontroli INTOSAI, nazywa się odpowiednimi, jeżeli są:

- *rzetelne*: wystarczające pod względem ilościowym i właściwe dla uzyskania wyników kontroli/audytu oraz bezstronne i wiarygodne. Wiarygodność dowodów kontroli/audytu zależy od ich charakteru, źródła oraz sposobu ich uzyskania,
- *stosowne*: odnoszące się do celów kontroli/audytu,
- *racjonalne*: koszt zebrania dowodów powinien proporcjonalny do wyników, które kontroler/audytor zamierza uzyskać.

Te przesłanki (dowody) są uzyskiwane jako wyniki badań, w szczególności badań technicznych – jednym z nich może być testowanie. Zbiór takich informacji

(wyników testów) może być podstawą do oceny parametrów jakościowych testowanego obiektu, w tym „bezpieczeństwa".

Wspomniane pozyskiwanie dowodów audytowych poprzez testy to nic innego jak, używając nieco bardziej technicznych określeń, diagnozowanie, a otrzymane wyniki składają się na diagnozę stawianą na zakończenie audytu. Przykładem takiej diagnozy może być np. stwierdzenie, że oceniany obiekt spełnia wymagania określone dla wskazanego poziomu EAL standardu Common Criteria (patrz [15]).

Wynikiem oceniania jest raport oceniającego, opisujący zastosowane procedury badawcze wraz z opisem i wynikami testów oraz dokładnie podanym czasem ich wykonania, zastosowanych w celu potwierdzenia lub zaprzeczenia istnienia określonych wad ocenianego systemu teleinformatycznego. Zwykle w raporcie oceniający podaje także sugestie jakie zidentyfikowane wady w jakiej kolejności należy usunąć.

Z ogólnej definicji audytu podanej we wstępie punktu wynika, że audyt jest szczególnym przypadkiem oceny. W publikacjach można znaleźć także następujące definicje audytu:

1. „ … systematyczny, niezależny i udokumentowany proces uzyskiwania dowodu z audytu oraz jego obiektywnej oceny w celu określenia stopnia spełnienia kryteriów audytu[2]".
2. „ … niezależny przegląd i badanie zapisów i działań przeprowadzane, by ocenić adekwatność systemowych mechanizmów kontrolnych, zapewnić zgodność z ustalonymi politykami i procedurami operacyjnymi oraz rekomendować konieczne zmiany w mechanizmach kontrolnych, politykach i procedurach[3]".
3. „ … *Audyt wewnętrzny* jest działalnością niezależną i obiektywną, której celem jest przysporzenie wartości i usprawnienie działalności operacyjnej organizacji. Polega na systematycznej i dokonywanej w uporządkowany sposób ocenie procesów: zarządzania ryzykiem, kontroli i ładu organizacyjnego, i przyczynia się do poprawy ich działania. Pomaga organizacji osiągnąć cele dostarczając zapewnienia o skuteczności tych procesów, jak również poprzez doradztwo[4]"

W Polsce obowiązujące objaśnienia znaczenia terminów związanych z audytem podaje opracowany przez Najwyższą Izbę Kontroli *Glosariusz* [16].

Instytut Audytorów Wewnętrznych (IIA), wyróżnia trzy podstawowe typy audytów: finansowy, zgodności i operacyjny. Wariantem audytu operacyjnego

[2] PN-EN ISO 9000:2001 – *Systemy zarządzania jakością. Podstawy i terminologia*. (starszą wersję normy przywołano celowo)

[3] *National Information Assurance* (IA) *Glossary*. The Committee on National Security Systems (US). June 2006.

[4] *https://www.iia.org.pl/o-nas/definicja-aw*, (dostęp 10.04.2017).

jest *audyt informatyczny*, tj. audyt wykorzystywanych w procesach biznesowych organizacji systemów informatycznych oraz projektów takich systemów. Cele wykonywania audytu informatycznego to przede wszystkim:

1. Weryfikacja zgodności działania systemów informatycznych z wymogami prawa (np. ustawą *o ochronie danych osobowych* lub *Krajowymi Ramami Interoperacyjności*).
2. Weryfikacja stanu bezpieczeństwa systemów informatycznych (w razie potrzeby także pojedynczych aplikacji) uwzględniająca skutki zidentyfikowanego ryzyka oraz zastosowane procedury kontrolne i ich efektywność.
3. Analiza ryzyka związanego z prowadzeniem projektu informatycznego.

Istotna, chociażby ze względu na koszty przedsięwzięcia i uzyskane wyniki, jest świadomość różnic pomiędzy audytem informatycznym a audytem bezpieczeństwa teleinformatycznego, który jest z kolei wariantem audytu informatycznego. Audyt bezpieczeństwa teleinformatycznego:

– nie dotyczy strony ekonomicznej stosowania środków informatyki w procesach biznesowych;

– nie obejmuje ryzyka związanego z prowadzeniem przez audytowaną organizację projektów z dziedziny informatyki – ocena taka jest zwykle częścią audytu informatycznego;

– nie obejmuje zwykle szczegółowego badania kodu aplikacji i spełnienia wymagań funkcjonalnych i operacyjnych – chyba, że jest to wyraźnie zaznaczone w umowie. Standardowo badany jest stopień zaaplikowania poprawek i uaktualnień likwidujących znane podatności.

Na ogólny, praktyczny schemat przeprowadzania audytu bezpieczeństwa teleinformatycznego (zgodny także z opisaną dalej metodyką LP-A), składają się następujące podstawowe czynności:

1. Rozpoznanie (środowiska, stanu posiadania, dokumentacji, procesów) badanej organizacji, np. podmiotu administracji publicznej.
2. Sporządzenie listy audytowej (*checklist*) według wybranego standardu – wzorca audytowego.
3. Wypełnienie listy audytowej z punktu 2 na podstawie ankietowania, wywiadów, wizji lokalnych, kontroli i analizy dokumentów audytowanej organizacji oraz wykonanych testów i badań. Spełnienie zaleceń poszczególnych punktów listy (w miarę potrzeb opatrzone komentarzami) jest kwalifikowane zwykle do jednej z następujących klas: *spełnione*, *nie spełnione*, *spełnione częściowo*, *nie dotyczy*.
4. Badania systemów ochrony fizycznej i technicznej (w tym systemów zasilania w energię elektryczną) oraz sieci i systemów teleinformatycznych

eksploatowanych w audytowanej organizacji. Badania te są przeprowadzane przy użyciu wyspecjalizowanych narzędzi i są uzupełniane testami penetracyjnymi.

5. Sporządzenie dokumentacji (raportu) z audytu, obejmującej udokumentowane przedsięwzięcia, wyniki i wnioski dla czynności z punktów 3 i 4. Dokumentacja końcowa musi być podpisana przez audytorów, imiennie gwarantujących rzetelność przeprowadzonej oceny.

Wykraczające poza ramy tego artykułu są pytania o to, jaki jest szczegółowy zakres audytu bezpieczeństwa teleinformatycznego, na ile jego przeprowadzenie może zakłócić normalną pracę organizacji oraz jakiego wsparcia ze strony audytowanej organizacji potrzebują audytorzy (pomocna może być tu metodyka LP-A).

Warto także zauważyć, że w informatyce termin „audyt", w sensie podanej wcześniej definicji, jest nadużywany. Często w konkretnych umowach z klientem lepiej byłoby używać terminu „ocena". Termin ten jest znacznie pojemniejszy i łączy się dobrze z terminem „wykonanie" (np. spisu inwentaryzacyjnego). Daje również pole do negocjowania z klientem jego rzeczywistych potrzeb.

Obecnie w środowiskach związanych z audytem informatycznym (głównie dla wariantu audytu – audytu wewnętrznego) toczą się dyskusje nt. przyszłości tego audytu i audytu bezpieczeństwa teleinformatycznego w szczególności oraz próbuje się opisać ujawniające się trendy. Dyskutowane zagadnienia są opisane w rozdziale 5.4 w [6].

6. Metodyka LP-A

Na metodykę LP-A wykonywania audytu bezpieczeństwa teleinformatycznego składają się opisy:

1) organizacji, zakresów kompetencji i kwalifikacji zespołu audytowego;
2) wyposażenia narzędziowego zespołu audytowego;
3) dokumentów niezbędnych do zainicjowania audytu oraz wytwarzanych podczas audytu;
4) modelu w postaci diagramów DFD (Data Flow Diagram) opisującego procesy wytwarzania dokumentów i powiązania pomiędzy nimi;
5) tzw. „dobrych praktyk", tj. heurystycznych sposobów postępowania, wypracowanych i sprawdzonych podczas dotychczasowej praktyki audytorskiej twórców metodyki.

Do przedstawienia procesów i przepływu dokumentów podczas audytu, zostały wykorzystane elementy metody strukturalnej projektowania systemów

informatycznych. Elementy te, to przede wszystkim tabele IPO (Input–Process–Output), i diagramy przepływu danych DFD.

Na podstawie metodyki LP-A można:

1) ocenić złożoność procesów składających się na audyt;
2) prześledzić zależności między dokumentami wytwarzanymi w procesie audytu;
3) dobrać skład zespołu audytowego, uwzględniając wymagane zakresy kompetencji (kwalifikacji i uprawnień) członków zespołu;
4) ocenić na podstawie zależności między procesami (oraz składu osobowego zespołu) możliwości równoległego prowadzenia zadań audytowych;
5) skonstruować harmonogram realizacji audytu (po uwzględnieniu konkretnych warunków wynikających z umowy ze zleceniodawcą);
6) oszacować koszty przeprowadzenia audytu (także z uwzględnieniem warunków umowy)

Opublikowana w 2003 roku metodyka [8], [4] była wynikiem doświadczeń i potrzeb związanych z pracami prowadzonymi w tamtym czasie przez jej autorów w zakresie audytów bezpieczeństwa teleinformatycznego. Metodyka została opracowana dla sprecyzowania i skrócenia dyskusji pomiędzy zleceniodawcą a potencjalnymi wykonawcami na temat „co jest do zrobienia" w pracach, w których zamówienie opiewało na „audyt bezpieczeństwa" lub „sprawdzenie stanu bezpieczeństwa" całości lub części systemu teleinformatycznego. Stwierdzono, że do efektywnego uzgadniania i prowadzenia przedsięwzięć audytowych jest niezbędne opracowanie metodyki, która wspomagałaby osiąganie następujących celów:

1. Opracowanie modelu referencyjnego czynności wykonywanych przez zespół audytowy. Jest on podstawą rozmów pomiędzy wykonawcami i zleceniodawcami o sposobie realizacji audytu z zakresu bezpieczeństwa informacyjnego.
2. Usystematyzowanie przedsięwzięcia audytowego w zakresie wzajemnej kolejności realizowanych czynności audytowych.
3. Usystematyzowanie przedsięwzięcia audytowego w zakresie generowanych w jego trakcie jak i niezbędnych do jego przeprowadzenia dokumentów.
4. Osiągnięcie komunikatywności i adaptowalności przez wykorzystanie takich mechanizmów formalnych, które:
   – Byłyby zrozumiale dla osób niemających wiedzy informatycznej (np. nieznających notacji graficznych typu UML i zasad obiektowości). Takie właściwości mają diagramy DFD i tablice IPO, które po krótkich wyjaśnieniach są zrozumiałe nawet dla laików.

– Byłyby proste w użyciu, w szczególności nie wymuszały stosowania narzędzi skomputeryzowanych.
– Byłyby łatwo skalowalne. Pierwotna wersja metodyki, opublikowana w [4] i [8] została rozwinięta do poziomu 3 diagramów DFD, ponieważ z doświadczeń autorów wynikało, że jest to wystarczający poziom szczegółowości do rozmów z kierownictwem i menedżerami potencjalnego zleceniodawcy audytu. Większa szczegółowość zaciemnia menedżerom (zleceniodawcy) obraz przedsięwzięcia audytowego szczegółami technicznymi. Mniejsza szczegółowość natomiast nie pozwala wykonawcom przedstawić zleceniodawcy potencjalnych problemów wynikających ze skali przedsięwzięcia i zaangażowanych po stronie zleceniodawcy zasobów mających istotny wpływ na czas i koszty prac.

Co prawda audyt, czyli badanie zgodności z pewnym wzorcem, nie odpowiada bezpośrednio na pytanie „czy jest bezpiecznie", ale rzetelne jego przeprowadzenie zwykle wymaga określenia jakości poszczególnych zabezpieczeń i jakości ich wdrożenia. Ocena ta może być prowadzona w różny sposób, ale autorzy metodyki **uznali techniczne badania bezpieczeństwa za podstawowy element takiej oceny**.

Szczegóły dotyczące rozpowszechnienia metodyki LP-A oraz jej modyfikacji w minionych piętnastu latach zainteresowany Czytelnik znajdzie w [9].

7. Wnioski

W artykule przedstawiono propozycję zintegrowanego podejścia do oceny stanu ochrony informacji w złożonych systemach informacyjnych. Współczesne trendy rozwoju takich systemów, jak „Internet Rzeczy" (IoT), łączenie sieci przemysłowych z sieciami biurowymi, „Big Data" itp. powodują, że ocena stanu ochrony zasobów informacyjnych związanych z takimi systemami, dotąd zwykle ograniczona do oceny stosowanych rozwiązań organizacyjnych i jakości stosowanego oprogramowania, przestaje być wystarczająca.

Podstawowe kryteria jakości „bezpieczeństwa" informacji, takie jak tajność, integralność i dostępność (to ostatnie kryterium w szczególności) zależą bowiem także od zastosowanych i eksploatowanych rozwiązań elektronicznych i elektromechanicznych nosicieli zasobów informacji i elementów je przetwarzających.

Elementem integrującym w przedstawionej koncepcji jest metodyka LP-A, której kluczowym elementem są badania techniczne prowadzone w ramach audytu bezpieczeństwa teleinformatycznego, dostarczające dowodów

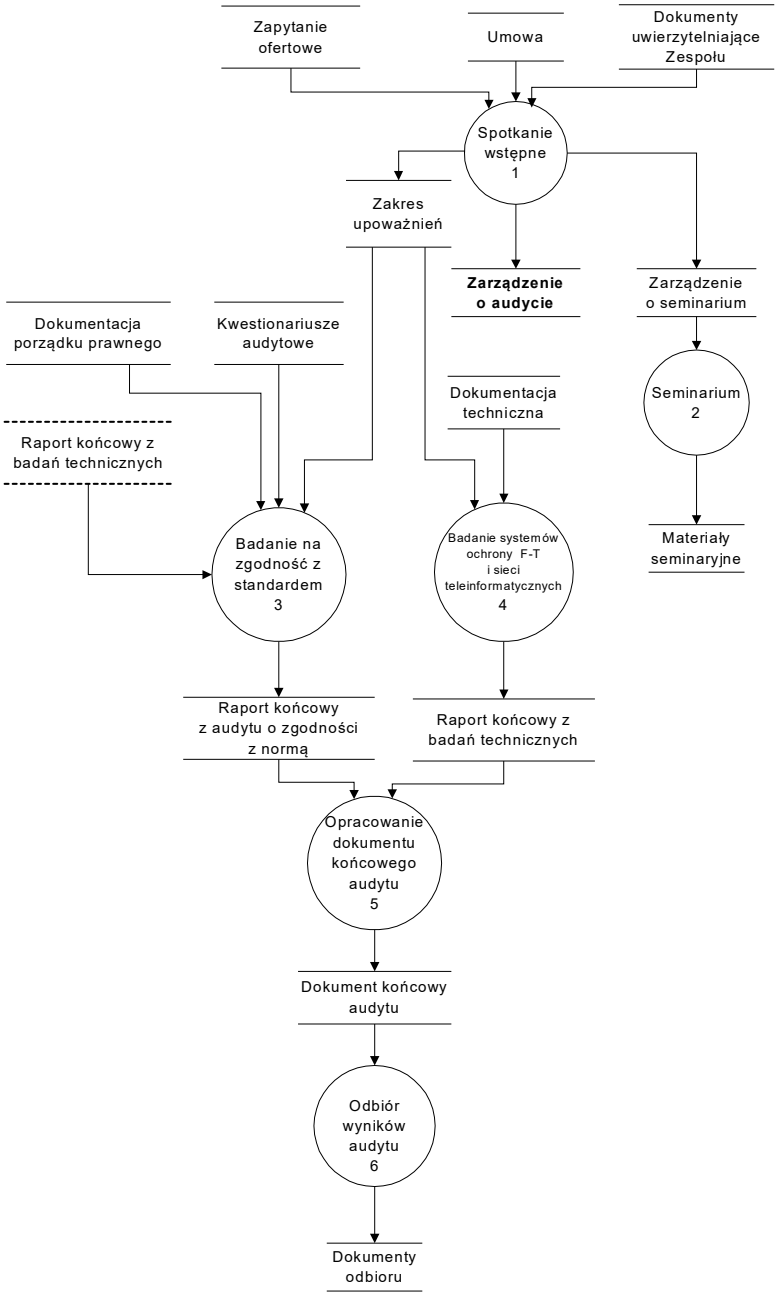

Diagram1: DFD_1 procesu audytu - schemat ogólny

Rys. 1. Diagram DFD procesu audytowego

audytowych o osiągnięciu celów stawianych przed zabezpieczeniami zasobów informacji.

Obecnie prowadzone są prace nad wsparciem metodyki LP-A o narzędzie typu „system ekspercki" (patrz definicja 4 i komentarz do niej), wspomagające diagnostykę techniczną prowadzoną na ścieżce technicznej audytu (patrz prawa strona diagramu na rys. 1).

Wejście	• zakresy upoważnień • dokumentacja techniczna sieci i systemów (teleinformatycznych i technicznych) Zleceniodawcy
Nr procesu	4 (*)
Proces	*badanie systemów ochrony fizycznej i technicznej oraz systemów i sieci teleinformatycznych Zleceniodawcy (ścieżka techniczna)*
Wyjście	raport końcowy z analiz i badań technicznych

Rys. 2. Tabela IPO metodyki LP-A – przykład

Literatura

[1] ANTCZAK M., ŚWIERCZYŃSKI Z., *Metodyki testowania bezpieczeństwa aplikacji internetowych*. Przegląd Teleinformatyczny, nr 2 (20), 2013, s. 13-38.

[2] ANTCZAK M., ŚWIERCZYŃSKI Z., *PTER - metodyka testowania bezpieczeństwa aplikacji internetowych*. Przegląd Teleinformatyczny, nr 1-2 (37), 2014, s. 35-68.

[3] BAYS M.E., *Metodyka wprowadzania oprogramowania na rynek*. WNT, Warszawa, 2002.

[4] LIDERMAN K., *Podręcznik administratora bezpieczeństwa teleinformatycznego*. MIKOM, Warszawa, 2003.

[5] LIDERMAN K., *Analiza ryzyka i ochrona informacji w systemach komputerowych*. PWN, Warszawa, 2008.

[6] LIDERMAN K., *Bezpieczeństwo informacyjne. Nowe wyzwania*. PWN, Warszawa, 2017.

[7] LIDERMAN K., *Informacyjna ciągłość działania i ataki na sieci różnych typów*. W: KOSIŃSKI J. (red.): *Przestępczość teleinformatyczna 2015*. WSPOL, Szczytno, 2015, s. 47-60.

[8] PATKOWSKI A.E., LIDERMAN K., *Metodyka przeprowadzania audytu z zakresu bezpieczeństwa teleinformatyczneg*o. Biuletyn ITA, nr 19, 2003, s. 3-49.

[9] PATKOWSKI A.E., LIDERMAN K., *Metodyka LP-A – dziesięć lat później*. Przegląd Teleinformatyczny, nr 2 (20), 2013, s. 65-79.

[10] PATKOWSKI A.E., *Metodyka P-PEN przeprowadzania testów penetracyjnych systemów teleinformatycznych*. Biuletyn ITA, nr 24, 2007, s. 63-96.

[11] ROZWADOWSKI T., *Diagnostyka techniczna obiektów złożonych*. WAT, Warszawa, 1983.

[12] ZIELIŃSKI Z., *Podstawy diagnostyki systemowej sieci procesorów o łagodnej degradacji i strukturze hipersześcianu*. WAT, Warszawa, 2013.

[13] COBIT®5: *Metodyka biznesowa w zakresie nadzoru nad technologiami informatycznymi w przedsiębiorstwie i zarządzania nimi (wersja polska)*. ISACA, 2012.

[14] IEC 61508: *Functional Safety: Safety-Related Systems*. IEC, 1995.

[15] www.commoncriteriaportal.org

[16] NIK: *Glosariusz terminów dotyczących kontroli i audytu w administracji publicznej*. Wyd.1. Warszawa, lipiec 2005.

Integrated testing and evaluation of the information protection

ABSTRACT: The paper presents a proposal of an integrated approach to the issues of assessing the state of information protection in complex information systems. The foundation of this proposal is technical diagnostics along with information security. Featured, among others issues of performing tests providing the basis for such an assessment: penetration tests and IT security audit. The last chapter of the paper briefly describes the LP-A methodology of performing an IT security audit that integrates various types of research, aiding various audit patterns, depending on the needs.

KEYWORDS: information protection, information security, diagnostics, audit, penetration tests, LP-A methodology.

Praca wpłynęła do redakcji: 10.06.2018 r.