DOI: 10.53122/ISSN.0452-5027/2021.1.12

Ustawa o KSC

Metody prowadzenia audytu cyberbezpieczeństwa

Ustawa o Krajowym Systemie Cyberbezpieczeństwa zdefiniowała tworzące go podmioty, w szczególności operatorów usług kluczowych, nakładając na nich obowiązek przeprowadzania regularnych audytów bezpieczeństwa systemu informacyjnego. Jednocześnie podkreśliła wagę wypracowania metody umożliwiającej ujednolicone podejście do raportowania wyników, minimalizujące tym samym subiektywizm oceny, sama jednak jej nie wskazując. Metodyka audytu bezpieczeństwa informacyjnego powinna spójnie łączyć wymogi ustawowe z normami i dobrymi praktykami. W artykule podjęto próbę usystematyzowania metod i standardów zarządzania cyberbezpieczeństwem, wykorzystując doświadczenia audytorów.

ADAM WYGODNY

Uwarunkowania prawne

Ustawę o Krajowym Systemie Cyberbezpieczeństwa[1] (dalej ustawa KSC), pierwszą, która kompleksowo określa jego ramy prawno-organizacyjne, Prezydent RP podpisał 1 sierpnia 2018 r. Jej przyjęcie było odpowiedzią na obowiązek implementacji dyrektywy Parlamentu Europejskiego i Rady (UE) w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[2] (*Network and Information Security Directive* – dyrektywa NIS). Celem – utworzenie efektywnego systemu bezpieczeństwa teleinformatycznego na poziomie krajowym[3]. Ustawa KSC definiuje operatorów usług kluczowych (UOK lub operatorzy) jako firmy i instytucje świadczące

[1] Ustawa z 5.7.2018 o Krajowym Systemie Cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560).
[2] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6.7.2016 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.
[3] K. Czaplicki, A. Gryszczyńska, G. Szpor: *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, Wolters Kluwer Polska, Warszawa 2019 r.

usługi o istotnym znaczeniu dla utrzymania krytycznej działalności społecznej lub gospodarczej. Wielu z nich posiadało już wcześniej sektorowe regulacje (sektor energetyczny, finansowy), które wymagały odpowiedniego przystosowania systemów informacyjnych. Ustawa objęła również nowe podmioty (sektor ochrony zdrowia, zaopatrzenia w wodę pitną), nieposiadające regulacji w tym obszarze.

Do 1 sierpnia 2020 r. wydano decyzje wyznaczające 163 UOK. Najwięcej wskazano w sektorze energii, a najmniej w sektorze zaopatrzenia w wodę pitną[4]. Ministerstwo Cyfryzacji szacuje docelową liczbę operatorów na ok. 500. Ustawa nakłada na nich obowiązek przeprowadzania regularnych audytów bezpieczeństwa informacyjnego. Pierwszy audyt powinien mieć miejsce po 12 miesiącach od otrzymania decyzji administracyjnej uznającej podmiot za operatora usługi kluczowej. Kolejne nie rzadziej niż raz na 2 lata. Za niewykonanie tych obowiązków przewidziano kary finansowe.

Bezpieczeństwem cyfrowym oraz związanymi z nim problemami zajął się Komitet Kontaktowy najwyższych organów kontroli (NOK) państw Unii Europejskiej, zrzeszający również Europejski Trybunał Obrachunkowy (ETO). W grudniu 2020 roku opublikował kompendium kontroli „Cyberbezpieczeństwo w UE i państwach członkowskich UE"[5]. Obecną edycję przygotował ETO we współpracy z NOK 12 państw członkowskich Unii: Danii, Estonii, Finlandii, Francji, Holandii, Irlandii, Litwy, Łotwy, Polski, Portugalii, Szwecji i Węgier. Najwyższa Izba Kontroli zaprezentowała w nim wyniki kontroli „Zapewnienie bezpieczeństwa działania systemów informatycznych wykorzystywanych do realizacji zadań publicznych"[6]. Kompendium zawiera również wyniki wybranych kontroli z tego obszaru przeprowadzonych przez pozostałe instytucje kontrolne uczestniczące w jego opracowaniu oraz przegląd inicjatyw strategicznych i uwarunkowań prawnych w dziedzinie cyberbezpieczeństwa UE.

Metodyka audytu

Ustawa KSC nie precyzuje metodyki przeprowadzenia audytu cyberbezpieczeństwa podmiotów kluczowych. Na rynku istnieje jednak wiele standardów i dobrych praktyk ułatwiających stworzenie ram audytu. Wypracowanie takiego wzorca, bazującego na standardach ISO 27001[7], zbiorze dobrych praktyk zarządzania procesami teleinformatycznymi (*Control Objectives for Information and related Technology* – COBIT) oraz zbiorze dobrych praktyk zarządzania usługami teleinformatycznymi

[4] M. Wrzosek: *Cyberbezpieczeństwo A.D. 2019*, Warszawa 2020 r., s. 20-22.

[5] *Kompendium kontroli Cyberbezpieczeństwo w UE i państwach członkowskich UE*, Unia Europejska, 2020 r.; <https://www.eca.europa.eu/sites/cc/Lists/CCDocuments/Compendium_Cybersecurity/CC_Compendium_Cybersecurity_PL.pdf>.

[6] Informacja o wynikach kontroli: *Zapewnienie bezpieczeństwa działania systemów informatycznych wykorzystywanych do realizacji zadań publicznych*, nr. ewid. 42/2016/P/15/042/KPB, Departament Porządku i Bezpieczeństwa Wewnętrznego NIK, kwiecień 2016; <https://www.nik.gov.pl/plik/id,10771,vp,13104.pdf>.

[7] International Standard ISO/IEC 27001:2019: *Information Technology – Security Techniques – Information Security Management Systems – Requirements*, Genewa 2019 r.

(*Information Technology Infrastructure Library* – ITIL) może usprawnić cały proces. Standardy i dobre praktyki w połączeniu z doświadczeniami charakterystycznymi dla danych sektorów pozwolą stworzyć narzędzia umożliwiające porównywanie wyników audytów przeprowadzanych niezależnie przez różne zespoły, działające w różnych sektorach UOK.

Planowanie audytu

Celem fazy planowania jest stworzenie programu, który szczegółowo opisuje obszary audytu cyberbezpieczeństwa OUK. Powinien zawierać wyniki wcześniejszej analizy przedaudytowej wraz z charakterystyką obszaru objętego kontrolą, najważniejszych uwarunkowań dotyczących badanej działalności OUK, analizę ryzyka wystąpienia nieprawidłowości oraz wyniki poprzednich audytów u tego operatora[8]. Wcześniej warto przeprowadzić „biały wywiad" oparty na źródłach jawnych (*Open Source Intelligence* OSINT). Do pozyskania informacji pochodzących z ogólnie dostępnych źródeł można wykorzystać gotowe narzędzia. Raport Polskiej Platformy Bezpieczeństwa Wewnętrznego[9] może być szczególnie pomocny w wyborze najlepszych rozwiązań. Rozpoznanie OSINT pozwala ustalić, czy OUK miał jakiekolwiek problemy z bezpieczeństwem teleinformatycznym oraz czy padł ofiarą cyberataków. Planując audyt warto zwrócić się do właściwego Zespołu Reagowania na Incydenty Bezpieczeństwa (*Computer Security Incident Response Team* – CSiRT) w celu ustalenia, czy kontrolowany OUK zgłaszał jakiekolwiek incydenty. Program audytu powinien określać w szczególności przedmiotowy i podmiotowy zakres, cel oraz mierniki umożliwiające dokonanie oceny kontrolowanej działalności[10].

Etap planowania audytu można podzielić na następujące fazy:

- zrozumienie biznesu;
- określenie regulacji i otoczenia prawnego;
- przegląd poprzednich audytów, OSINT;
- identyfikacja polityk, standardów i procedur;
- przeprowadzenie analizy ryzyka;
- ustalenie zakresu i celów audytu;
- opracowanie strategii i programu;
- wyznaczenie zasobów;
- ustalenie planu realizacji zadań.

Program audytu

Program audytu to zestaw dokumentów określających jego cele, oczekiwane wyniki, identyfikujący procesy zarządzania ryzykiem, a także zawierający ocenę ryzyka. Przygotowując program audytor powinien poznać strategię i cele biznesowe podmiotu kluczowego, zidentyfikować ryzyko[11] i na tej podstawie nadać priorytety obszarom i procesom podlegającym audytowi. Procesom o wysokim ryzyku należy nadać wysoki priorytet.

Program audytu powinien odnosić się do modelu CIA (*Confidentiality, Integrity,*

[8] E. Jarzęcka-Siwik, B. Skwarka: *Komentarz do ustawy o Najwyższej Izbie Kontroli*, Difin, Warszawa 2017 r., s. 121-124.
[9] *Oprogramowanie i narzędzia wspomagające analizę kryminalną*, Raport Polskiej Platformy Bezpieczeństwa Wewnętrznego, Warszawa 2019 r.
[10] E. Jarzęcka-Siwik, B. Skwarka: *Komentarz do ustawy*…, op.cit., s. 122.
[11] *Risk IT Practitioner Guide*, USA, 2009 r.

Availability – CIA), który stworzono do kierowania polityką bezpieczeństwa informacji w firmie. Poufność (*Confidentiality*) oznacza, że informacja powinna być dostępna jedynie dla podmiotów do tego upoważnionych; integralność (*Integrity*), że wszelkie nieuprawnione modyfikacje informacji są niedozwolone. Dostępność (*Availability*) to gwarancja uzyskania dostępu do informacji w każdych okolicznościach, przewidzianych w polityce bezpieczeństwa informacji. Program audytu jest więc swojego rodzaju inteligentną nawigacją, która prowadzi audytorów przez cały projekt w sposób najbardziej optymalny i skuteczny. Pokazuje nie tylko najszybszą drogę, ale również definiuje potencjalne zagrożenia i niezbędne zasoby. Wynikiem końcowym jest dostarczenie zainteresowanym raportu i wniosków pokontrolnych. Dobrą praktyką w trakcie układania programu jest korzystanie ze standardu – System Zarządzania Bezpieczeństwem Informacji ISO 2700[12]. Podstawą są oczywiście powszechnie obowiązujące przepisy prawa i regulacje resortowe, które dotyczą danego operatora.

Oto jak mogą zostać ukształtowane kolejne fazy przygotowania programu audytu:
- analiza celów biznesowych i regulacji,
- identyfikacja ryzyka,
- określanie obszarów priorytetowych,
- mapowania obszarów modelu CIA,
- definiowanie sposobów pozyskiwania informacji,
- określenie szczegółowych pytań,
- zdefiniowanie kryteriów oceny,
- wyznaczenie struktury organizacyjnej audytu,
- identyfikacja interesariuszy.

Struktura organizacyjna audytu

Kluczowym elementem decydującym o rzetelności audytu są kwalifikacje i sposób pracy członków zespołu audytowego[13]. Ustawa KSC wskazuje, że powinno być minimum dwóch niezależnych audytorów z określonymi kompetencjami i uprawnieniami. Pozwala to na krzyżową kontrolę realizacji zadań (tzw. *cross checking*). Zewnętrzni audytorzy mają o wiele szersze spojrzenie na organizację. Doświadczenie pozwala im pozycjonować OUK względem innych operatorów działających w tym samym sektorze. Audytorzy powinni posiadać pełną niezależność, umocowania prawne i uprawnienia wewnątrz organizacji OUK do przeprowadzenia audytu. Organem struktury organizacyjnej, który wspiera realizację ich zadań jest komitet sterujący[14]. W jego skład powinien wchodzić przedstawiciel zarządu OUK, przedstawiciele biznesu, działu bezpieczeństwa oraz działu teleinformatycznego. W ramach struktury organizacyjnej powinni być zdefiniowani interesariusze, którzy będą odbiorcami końcowymi raportu i rekomendacji poaudytowych. Złożoność badanych obszarów może powodować, że do zespołu audytowego zostaną powoływani niezależni eksperci.

[12] International Standard ISO/IEC 27001:2019: *Information Technology*…, op.cit.
[13] K. Liderman: *Bezpieczeństwo informacyjne. Nowe Wyzwania*, PWN, Warszawa 2017 r., s. 383.
[14] K. Bradley: *Podstawy metodyki Prince 2*, CRM, Warszawa 2002 r., s. 28-32, 152-155.

Obszary audytu

Określenie obszarów prowadzenia audytu powinno odbywać się indywidualnie dla danego OUK. W metodyce COBIT 5[15] zdefiniowano siedem kategorii obszarów umożliwiających przeprowadzenie skutecznego audytu: zasady, polityka i metodyka; procesy; struktury organizacyjne; kultura, etyka i zachowanie; informacja; usługi, infrastruktura i aplikacje; ludzie, umiejętności i kompetencje.

W dalszej części przedstawiono obszary, które najczęściej pojawiają się w programie audytu cyberbezpieczeństwa, w części są one zgodne z metodyką COBIT 5 oraz pokrywają się z obszarami określonymi w ustawie KSC. W zależności od specyfiki OUK i segmentu rynku, w którym działa, obszary mogą nieznacznie różnić się istotnością lub pojawiać się nowe.

Struktura organizacyjna UOK

Struktura organizacyjna OUK, ukierunkowana i wspierająca realizację zadań związanych z cyberbezpieczeństwem, to kluczowy element skutecznej ochrony i zapobiegania cyberatakom. Prowadząc audyt powinno się ją szczegółowo przeanalizować i zweryfikować czy działy teleinformatyczne (IT) i bezpieczeństwa są wystarczająco odseparowane. Często te zespoły funkcjonują w ramach jednego departamentu, co nie jest dobrą praktyką. Dział bezpieczeństwa powinien przedstawiać raporty bezpośrednio zarządowi, podczas gdy dział IT dyrektorowi IT. Należy również zwrócić uwagę na role pracowników wykonujących zadania związane z cyberbezpieczeństwem. Warto zweryfikować, czy w ramach struktur działu bezpieczeństwa powołana jest scentralizowana jednostka zajmująca się kwestiami bezpieczeństwa na poziomie organizacyjnym i technicznym (*Security Operations Center* – SOC). Kluczowe jest ustalenie, czy uprawnienia do podejmowania decyzji i akceptacji posiada tylko jedna osoba. Takie przypisanie uprawnień może powodować ryzyko nadużyć oraz wstrzymanie procesu w przypadku nagłej nieobecności pracownika. Dodatkowo należy zwrócić uwagę, czy ktokolwiek w OUK ma nieograniczony dostęp do wszystkich danych oraz jak szybko wykrywane są błędy pracowników.

Analizując organizację OUK dobrze jest też sprawdzić, czy są tam tylko osoby zatrudnione na etacie, czy również zewnętrzni pracownicy kontraktowi. W przypadku tych ostatnich należy zwrócić uwagę, jak ujęto w ich umowach zapisy o poufności i przestrzeganiu polityki bezpieczeństwa OUK. Umowy jasno powinny precyzować zakres praw i obowiązków takich osób oraz sposób, w jaki otrzymują oni dostęp do danych systemu informacyjnego operatora. Realizacja usług przez pracowników kontraktowych oraz również przez dostawców w ramach wdrażanych projektów powinna mieć jasno zdefiniowany poziom jakości usług informatycznych (*Service Level Agreement* – SLA)[16]. OUK powinien posiadać

[15] *COBIT 5 – Metodyka biznesowa w zakresie nadzoru nad technologiami informatycznymi w przedsiębiorstwie i zarządzania nimi*, ISACA, 2012 r., s. 65-85.
[16] Axelos, *ITIL Foundation – v4*, TSO, 2019 r.

narzędzia i procedury do jego skutecznego monitorowania i egzekwowania.

W ramach audytu struktury organizacyjnej dobrze jest też przeanalizować, czy operator posiada wewnętrzne struktury audytorskie i czy osoby do tego wyznaczone regularnie prowadzą wewnętrzny audyt. Wyniki takich postępowań mogą być przydatne w czasie audytu cyberbezpieczeństwa OUK.

Polityka cyberbezpieczeństwa

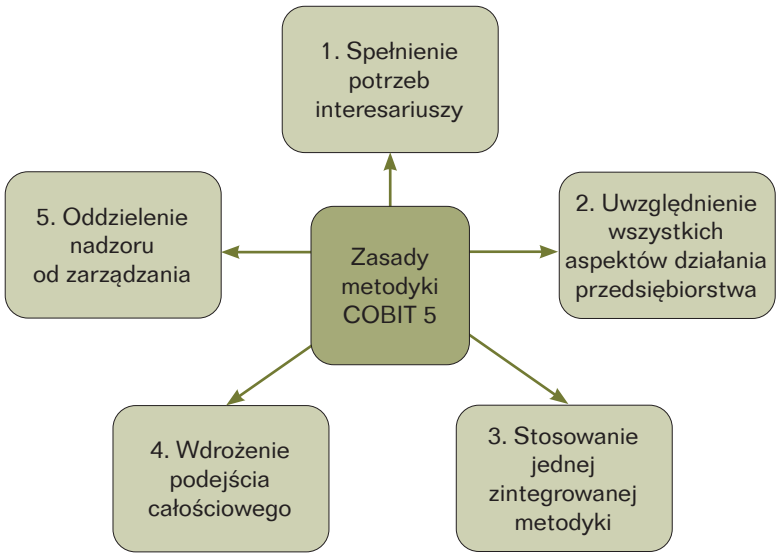
System ochrony informacji OUK powinien być udokumentowany i sformalizowany przez: politykę cyberbezpieczeństwa, plany, instrukcje i procedury przebiegu procesów. Polityka bezpieczeństwa określa zorganizowane działania mające doprowadzić do osiągnięcia zakładanych celów[17]. Powinna również wskazywać wymogi dotyczące danego OUK. Rozporządzenie Rady Ministrów do ustawy KSC[18] określa rodzaje i zawartość dokumentacji cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej. Wymienia dokumentację normatywną (dotyczącą systemu zarządzania bezpieczeństwem informacji, ochrony fizycznej, systemu zarządzania ciągłością działania), techniczną (systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej) oraz operacyjną (procedury, instrukcje, opisy wykonywania czynności). OUK powinien stworzyć, wdrożyć i aktualizować dokumentację zarówno na poziomie normatywnym, jak i operacyjnym. Przygotowując się do audytu warto sporządzić ankiety do każdego z systemów informacyjnych wspierających realizację usług kluczowych, których wypełnienie pomoże wskazać odpowiednią dokumentację. W czasie audytu należy przeprowadzić wywiady z pracownikami sprawdzające ich znajomość dokumentacji cyberbezpieczeństwa. Każdy pracownik powinien znać i przestrzegać polityki bezpieczeństwa organizacji, wiedzieć gdzie szukać informacji szczegółowych dotyczących konkretnych procesów. Przeprowadzając analizę warto zwrócić uwagę na metryczki dokumentów i zbadać dowody potwierdzające systematyczne aktualizacje.

Nadzór nad cyberbezpieczeństwem

Kontrola ma kluczowe ma znaczenie również w systemie organizacji cyberbezpieczeństwa OUK. Operator może posiadać doskonale wyszkoloną kadrę, strategię i politykę bezpieczeństwa, precyzyjnie opisujące każdy proces w organizacji, posiadać najnowocześniejszą technologię i plany ciągłości działania (*Business Continuity Planning* –BCP), jeżeli jednak nie sprawuje właściwego nadzoru nad realizacją tych zadań, wszystkie te narzędzia mogą być nieskuteczne. Badając nadzór nad cyberbezpieczeństwem OUK dobrze jest sięgnąć do standardów i dobrych praktyk (COBIT, ITIL). W czasie wywiadu z pracownikami dobrą praktyką jest sprawdzenie, co myślą o opisanych procedurach, jak oceniają ich realizację. Analizując dokumenty należy sprawdzić, czy są aktualne, czy wskazano czemu służą oraz w jaki

[17] K. Liderman: *Bezpieczeństwo informacyjne…*, op.cit., s. 224-234.
[18] Ustawa z 5.7.2018 o Krajowym Systemie Cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 2080).

Rysunek 1. **Zasady metodyki COBIT 5**



Źródło: Opracowanie na podstawie ISACA: *COBIT 5 – Metodyka biznesowa w zakresie nadzoru nad technologiami informatycznymi w przedsiębiorstwie i zarządzania nimi*.

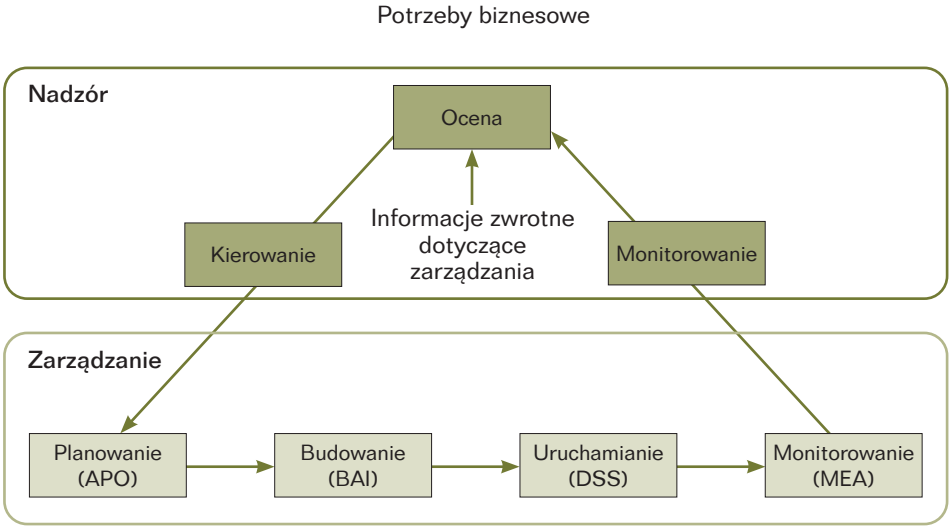
sposób są dystrybuowane, jak skuteczny jest proces komunikacji. Metodyka COBIT 5 definiuje nadzór nad technologiami informacyjnymi i zarządzanie nimi w sposób całościowy, w odniesieniu do wszystkich aspektów działalności OUK[19].

Nawet jeżeli nadzór nad systemem cyberbezpieczeństwa OUK nie został zbudowany zgodnie z metodyką COBIT, dobrze jest wykorzystać ją do przeprowadzenia audytu tego obszaru według wspomnianych wcześniej pięciu podstawowych zasad. Sprawdzając nadzór należy zweryfikować, czy organizacja, procesy i polityki wspierają potrzeby biznesowe interesariuszy oraz czy zachowana jest równowaga między osiąganiem korzyści, optymalizacją ryzyka i wykorzystaniem zasobów. Organizacja IT powinna wspierać budowanie przewagi konkurencyjnej przedsiębiorstwa. Nie może spowalniać tych procesów. Powinien zostać wypracowany kompromis wspierający cele biznesowe organizacji.

W metodyce COBIT 5[20] nadzór nad technologiami informatycznymi w przedsiębiorstwie jest częścią ładu korporacyjnego. Obejmuje nie tylko procesy IT, ale wszystkie funkcje i procesy realizowane przez OUK. Traktuje informacje i związane

[19] *COBIT 5 – Metodyka biznesowa w zakresie nadzoru…*, op.cit., s. 13.
[20] *COBIT 5 – Metodyka biznesowa w zakresie nadzoru…*, op.cit., s. 14

Rysunek 2. **Kluczowe obszary nadzoru i zarządzania w ramach metodyki COBIT 5**



Źródło: Opracowanie na podstawie ISACA: *COBIT 5 – Metodyka biznesowa w zakresie nadzoru nad technologiami informatycznymi w przedsiębiorstwie i zarządzania nimi*.

z nimi technologie jako aktywa podlegające ochronie i wymagające uwzględnienia przez wszystkich pracowników przedsiębiorstwa. Metodyka COBIT 5 jest spójna z innymi stosowanymi standardami i metodykami. Pomaga stworzyć nadrzędną strukturę nadzoru nad technologiami informatycznymi i zarządzania nimi.

Prowadząc audyt procesów nadzoru nad cyberbezpieczeństwem u operatora kluczowego należy zwrócić uwagę, czy jest skuteczny i został wyraźnie oddzielony od zarządzania. Nadzór i zarządzanie obejmuje działania o odmiennym charakterze, wymagające różnych struktur organizacyjnych i służące różnym celom.

Dzięki nadzorowi OUK zyskuje pewność, że oceniono potrzeby interesariuszy, aby jak najlepiej określić zrównoważone cele przedsiębiorstwa. Nadzór polega również na ukierunkowaniu działań przez nadanie priorytetów i podejmowanie decyzji oraz na monitorowaniu sprawności i zgodności działań z obranym kierunkiem i celami szczegółowymi. Zgodnie z metodyką COBIT, w większości przedsiębiorstw za właściwy nadzór odpowiada zarząd firmy. Poszczególne obowiązki mogą zostać przekazane specjalnym strukturom organizacyjnym.

Zarządzanie natomiast polega na planowaniu, budowaniu, realizacji i monitorowaniu działań w sposób spójny z kierunkiem wskazanym przez organ nadzorujący, aby osiągnąć cele przedsiębiorstwa. Związane z tym obowiązki najczęściej powierza się kadrze zarządzającej, podlegającej dyrektorowi generalnemu, który odpowiada przed zarządem.

Prowadząc audyt nadzoru należy zweryfikować czy wspomniane zależności zostały właściwie określone w danej organizacji. Trzeba również odnieść się do trójkąta CIA i zbadać w jaki sposób sprawowany jest nadzór nad poufnością, integralnością i dostępnością systemu informacyjnego OUK. Ważne jest, aby istniały dowody, że ma on stale miejsce. Pomocne mogą tu być wywiady z pracownikami i uzyskiwanie ich opinii na temat funkcjonowania nadzoru.

Kompetencje i szkolenia

Audyt obszaru kompetencji i szkoleń powinien zweryfikować przygotowanie pracowników odpowiedzialnych za zadania związane z cyberbezpieczeństwem OUK – czy posiadają wymaganą wiedzę, certyfikaty i doświadczenie niezbędne do realizacji zadań. Wzorcem, do którego można się odnieść badając ten obszar, może być opracowanie Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), która stworzyła mapę kompetencji dla sektora publicznego i współtworzy proces certyfikacji oraz współpracuje z uczelniami wyższymi na terenie UE[21]. Przydatne mogą okazać się również doświadczenia organizacji komercyjnych, takich jak: CompTIA, ISACA, ISC2, które prowadzą certyfikację specjalistów związanych z cyberbezpieczeństwem.

Badając ten obszar warto przeanalizować ścieżki rozwoju pracowników. Na rynku wciąż brakuje specjalistów z cyberbezpieczeństwa. Ważne, aby OUK potrafił zadbać o zatrzymanie wyszkolonej kadry i posiadał skuteczne systemy motywujące oraz zapewniające im rozwój osobisty. Jest to kluczowe z punktu widzenia celu działań operatora i powinno podlegać audytowi. Warto przeanalizować więc rotację pracowników, systemy oceny pracowniczej i rozwoju. W obszarze kompetencje i szkolenie powinna również znajdować się analiza realizacji szkoleń z zakresu cyberbezpieczeństwa, tj. budowania świadomości wśród wszystkich pracowników OUK. Ważna jest regularność szkoleń, organizowanych nie tylko przy okazji zatrudniania nowych osób. Budowanie świadomości powinno być połączone z praktycznymi ćwiczeniami i symulacjami ataków.

Analiza ryzyka

Analiza i ciągłe zarządzanie ryzykiem to kluczowy element realizowany przez OUK w ramach świadczenia usługi kluczowej. Tak naprawdę zarządzanie cyberbezpieczeństwem sprowadza się do zarządzania ryzykiem. Dostrzega to również Ministerstwo Cyfryzacji, które dąży do opracowania wspólnej metodyki i narzędzi zarządzania ryzykiem. Nie chodzi o kolejny wymóg regulacyjny, a raczej o określenie wspólnego sposobu szacowania ryzyka. Takie narzędzie pozwoliłoby na łatwe porównywanie wyników analiz oraz stworzenie obrazu ryzyka wspólnego dla operatorów.

Ustawa KSC[22] nakłada na OUK obowiązek regularnego szacowania ryzyka wystąpienia incydentu oraz zarządzania

[21] *Cybersecurity skills development in the EU*, ENISA, Greece 2020 r.
[22] Art. 8.1. Ustawy z 5.7.2018 o Krajowym Systemie Cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560).

nim. Polityka bezpieczeństwa operatorów powinna jasno definiować struktury odpowiedzialne za realizację tych zadań. Zarządzanie ryzykiem powinno być procesem ciągłym, stale doskonalonym, zmierzającym do zminimalizowania jego wystąpienia. Służą temu techniczne, organizacyjne i operacyjne mechanizmy zabezpieczające. Wybór adekwatnych metod powinien opierać się na istotności i roli systemów informacyjnych. Prowadząc audyt należy zwrócić uwagę na dokumentację bezpieczeństwa systemów wykorzystywanych do realizacji usług kluczowych. Polityka bezpieczeństwa musi określać sposób i cykliczność przeprowadzania analiz ryzyka związanych z zapewnieniem poufności, integralności i dostępności systemu informacyjnego OUK. Ważne jest, by były przeprowadzane nie tylko przed uruchomieniem lub aktualizacją danego systemu. Operator powinien regularnie szacować ryzyko i posiadać dokumentację potwierdzającą ciągłość tego procesu.

W trakcie audytu warto również zwrócić uwagę na jakość danych wykorzystanych do analizy ryzyka. Czy jest oparta na bazie wiedzy i danych tylko od analityka, czy raczej pochodzi z całej organizacji UOK. W wielu organizacjach analizę ryzyka poprzedza się ankietami kierowanymi do szerokiego grona użytkowników, administratorów i właścicieli (gestorów) systemu.

Analiza ryzyka składa się z kilku faz: planowania, zbierania informacji, identyfikacji zagrożeń i podatności na nie, kalkulacji oraz analizy kosztów i określenia adresatów ryzyka. W fazie planowania OUK powinien utworzyć zespoły, zidentyfikować zakres, narzędzia i metodologię analizy ryzyka oraz ustalić akceptowalne jego poziomy. W fazie zbierania informacji operator może skupić się na identyfikacji kluczowych zasobów (infrastruktura, dane, tajemnice przedsiębiorstwa, dane klientów, informacje wpływające na reputację OUK). Do zdefiniowanych zasobów należy przypisać wartości, na które składa się m.in. koszt wymiany lub akwizycji, koszt i czas wytworzenia zasobu, koszt serwisu oraz odpowiedzialność w przypadku braku ochrony zasobu. Następnie OUK musi szczegółowo określić podatności i zagrożenia mające wpływ na zasoby i na tej podstawie skalkulować ryzyko.

Metodologia powinna zawierać podejście ilościowe (numeryczne, walutowe) i jakościowe (oparte na opiniach, scenariuszach, systemach ratingowych). Kalkulacja musi obejmować spodziewaną jednorazową stratę (SLE), czyli wyrażoną w pieniądzach stratę z jednego incydentu. Współczynnik SLE jest iloczynem wartość zasobu i współczynnika ekspozycji (narażenia). Kolejnym współczynnikiem istotnym w kalkulacji ryzyka jest roczny wskaźnik zdarzeń (ARO). Definiuje oczekiwaną liczbę wystąpień danego zagrożenia w ciągu jednego roku. Jeżeli spodziewamy się, że dane niebezpieczeństwo może zdarzyć się raz na 20 lat (np. pandemia), to ARO będzie wynosić 1/20. Dla zdarzenia zachodzącego często, na przykład spodziewane pojawienie się wirusa w sieci, ARO może przybierać duże wartości. Biorąc pod uwagę możliwość pojawienia się nowych wirusów 2 razy w miesiącu, ARO jest szacowane na poziomie 24 (2 nowe wirusy × 12 miesięcy w roku). Iloczyn współczynników SLE i ARO wylicza spodziewaną stratę roczną (ALE).

Mając wyliczoną wartość spodziewanej rocznej straty, OUK powinien planować budżet na rozwiązania dotyczące bezpieczeństwa. Roczny koszt zabezpieczenia zawsze powinien być niższy od ALE. Jeżeli wartość zabezpieczeń przekracza wartość straty, to mamy do czynienia z niegospodarnością i niecelowością działań OUK. Oczywiście w niektórych sytuacjach takie działanie może być uzasadnione, np. w przypadku gdy utrata reputacji organizacji jest wyższa niż wysoki koszt wdrożenia zabezpieczeń. Audyt powinien również zbadać ten element analizy ryzyka przeprowadzanej przez OUK. Zdefiniowanym rodzajom ryzyka zawsze muszą odpowiadać konkretne działania zapobiegawcze, transformacje (ubezpieczenia), świadoma akceptacja lub unikanie. Analiza ryzyka często traktowana jest przez OUK jako wymóg regulacyjny, dokonywany tylko przy projektowaniu systemu. Wprowadzenie cykliczności analizy w połączeniu z wykorzystywaniem wyników i mapowaniem tych danych z systemem zrównoważonej karty wyników (*Balanced Scorecard*) może skutecznie budować przewagę konkurencyjną. Decyzja o zaakceptowaniu zidentyfikowanego ryzyka jest całkowicie do przyjęcia, natomiast zignorowanie ustaleń bez jakiejkolwiek oceny jest dużym zaniedbaniem[23].

Usługi, infrastruktura i aplikacje

Złożoność technologiczna infrastruktury, aplikacji i usług z tym związanych może stanowić pewnego rodzaju wyzwanie dla audytora. Przy realizacji zadań nie jest wymagana szczegółowa wiedza dotycząca technologii. Ważne jednak, żeby audytor był świadomy ich istnienia i dobrych praktyk wykorzystania. Wszędzie tam, gdzie jest wymagane głębsze zbadanie rozwiązań i technologii, audytor powinien powoływać niezależnych ekspertów i wykorzystywać ich raporty oraz opinie. Do niedawna technologia była przewagą konkurencyjną. Organizacje nieustannie zwiększały budżety i inwestowały w nadziei, że uchroni je to przed cyberatakami. Oczywiście technologia nadal jest ważna, ale nie stanowi już przewagi konkurencyjnej. Powszechność narzędzi do cyberataków, dostępność usług hackerskich w modelu *Hack as a Service* powoduje, że mamy do czynienia z coraz większą liczbą ataków. Nie jest już kwestią, czy zostaniemy zaatakowani, lecz raczej kiedy. Ma miejsce swego rodzaju transformacja, polegająca na odejściu od inwestycji technologicznych na rzecz przygotowania operacyjnego na wypadek cyberataku. Działania audytowe powinny więc koncentrować się na sposobie zapewnienia poufności, integralności i dostępności infrastruktury i aplikacji.

Ważne, aby OUK określał w dokumentacji cyberbezpieczeństwa sposób wprowadzania systemów, prowadził ich rejestr, posiadał politykę dostępu do danych, przy zachowaniu zasady nadawania minimalnych uprawnień tylko do niezbędnych zasobów. Przy przeglądzie tego obszaru warto zwrócić uwagę, czy istnieje dokumentacja i pliki

[23] C. Dotson: *Bezpieczeństwo w chmurze. Przewodnik po projektowaniu i wdrażaniu zabezpieczeń*, PWN, Warszawa 2020 r., s. 107.

konfiguracyjne dla urządzeń, czy są bezpiecznie przechowywane i opisane w bazie danych zarządzania konfiguracją (*Configuration Management Data Base* – CMDB). Ważne jest zweryfikowanie, czy OUK używa tylko systemów i aplikacji, które wcześniej zostały zdefiniowane i dopuszczone do użytkowania. Celem audytu cyberbezpieczeństwa OUK nie jest przeprowadzanie testów penetracyjnych, ale raczej sprawdzenie, czy operator regularnie podejmuje takie działania i wdraża rekomendacje potestowe.

Zarządzanie incydentem

Ustawa KSC[24] nakłada na operatora obowiązek monitorowania systemu informacyjnego w trybie ciągłym. Często do monitoringu i zbierania logów ze wszystkich systemów operatorzy wykorzystują systemy klasy SIEM (*Security Information and Event Management*), które dodatkowo mogą być wspierane systemami SOAR (*Security Orchestration, Automation And Response*). Ustawa KSC nakłada obowiązek zbierania informacji o zagrożeniach cyberbezpieczeństwa i podatności na incydenty[25]. Incydenty powinny być obsługiwane, co oznacza ich wykrywanie, rejestrowanie, analizę, prowadzenie działań prewencyjnych oraz minimalizujących negatywne skutki[26]. Do działań prewencyjnych często wykorzystywany jest system informacji o zagrożeniach w cyberprzestrzeni (*Cyber Threat Intelligence* – CTI). Analizy przeprowadzane dzięki narzędziom CTI pozwalają poznać „wroga", uzyskać wiedzę o taktyce i technikach wykorzystywanych przez atakującego. Uzyskane informacje ułatwiają ocenę czy OUK posiada potencjał do wykrycia ataku i skutecznej obrony. CTI nie może ograniczać się tylko do analizy alertów. Musi analizować wszystkie procesy biznesowe operatora usługi kluczowej. W czasie audytu warto zweryfikować, czy OUK aktywnie używa CTI oraz w jaki sposób operacyjnie wykorzystuje pozyskaną wiedzę.

KSC[27] podkreśla obowiązek zarządzania incydentem przez OUK. Często do realizacji tych zadań operatorzy powołują zespoły SOC (*Security Operations Center*), które pracują w trybie 7/24. Dobrą praktyką w budowaniu SOC i organizacji zarządzania incydentami jest wykorzystanie standardu ITIL. Skuteczna realizacja zadań wynikająca z zarządzania incydentami powinna obejmować cały cykl istnienia incydentu, począwszy od identyfikacji, przez kwalifikację i reagowanie, a kończąc na zamknięciu i raportowaniu wniosków.

W ramach okresowej, corocznej weryfikacji poprawności i skuteczności działań SOC operator usługi kluczowej powinien wprowadzić regularne testy procedur (symulacje wystąpienia incydentu). Incydenty muszą być klasyfikowane według zasad opisanych w dokumentacji bezpieczeństwa OUK. Kanał komunikacji i procedura zgłaszania naruszeń bezpieczeństwa powinny

[24] Art. 8.2. Ustawy z 5.7.2018 o Krajowym Systemie Cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560).
[25] Art. 8.3. Ustawy z 5.7.2018 o Krajowym Systemie..., op.cit.
[26] K. Liderman: *Bezpieczeństwo informacyjne…*, op.cit., s. 51-64.
[27] Art. 8.4. ustawy KSC, Dz.U. z 2018 r. poz. 1560.

Rysunek 3. **Postępowanie po wystąpieniu incydentu**

Źródło: Opracowanie własne.

być sformalizowane i obejmować również obowiązki regulacyjne. Przykładowo, incydenty poważne, którymi według Ministerstwa Cyfryzacji są te, które powodują poważne obniżenie jakości lub przerwanie realizacji świadczenia usługi kluczowej, należy zgłaszać do właściwego CSIRT w ciągu 24 godzin[28].

Warto też zwrócić uwagę, czy obsługa incydentów dokumentowana jest w jednym miejscu, czy jest ustalony czas reakcji i mierzony czas jego obsługi. W ramach zarządzania incydentami OUK powinien posiadać zdefiniowane procesy zbierania dokumentacji dowodowej w ramach kryminalistyki cyfrowej. Wewnętrzne struktury SOC muszą współpracować ze sobą na poziomie wielu OUK z tego samego sektora. Obecnie CSIRT dla sektora usług finansowych funkcjonuje przy Komisji Nadzoru Finansowego. Przy Ministerstwie Klimatu powołano sektorowy Zespół Udostępniania Informacji i Analiz *Information Sharing and Analysis Centre* (ISAC) dla operatorów z sektora energetycznego. Dobrą praktyką jest powoływanie podobnych zespołów w innych sektorach. Współpraca i wymiana informacji, wspólna baza zagrożeń skutecznie zwiększa odporność na cyberataki i łagodzi skutki ich wystąpienia.

Zarządzanie tożsamością i dostępem

System zarządzania cyberbezpieczeństwem OUK, zgodnie z ustawą KSC[29], powinien obejmować bezpieczeństwo fizyczne i środowiskowe, uwzględniające kontrolę dostępu. Bezpieczeństwo fizyczne obejmuje: ochronę fizyczną obiektu OUK, monitoring wizyjny i system kontroli dostępu. Kontrola dostępu środowiskowego powinna zawierać mechanizmy identyfikacji, oceny autentyczności i autoryzacji użytkownika. Identyfikacja może opierać się na unikalnej nazwie użytkownika, często kombinacji imienia i nazwiska. Dobrą praktyką jest stosowanie wieloelementowej oceny autentyczności, która stanowi kombinację kilku technik. Autoryzacja jest nadaniem uprawnień do podejmowania określonych działań we wskazanych obiektach lub podmiotach. Jej celem jest kontrola dostępu, która potwierdza, czy dany podmiot jest uprawniony do korzystania z żądanego zasobu. Kontrola dostępu jest kluczowa z perspektywy ochrony przed utratą poufności, integralności i dostępności.

[28] Art. 11.1. Ustawy z 5.7.2018 o Krajowym Systemie..., op.cit.
[29] Art. 8.2. Ustawy z 5.7.2018 o Krajowym Systemie..., op.cit.

Dostęp do zasobów powinien być przydzielany na zasadzie minimalnych uprawnień, niezbędnych do realizacji zadań. Prowadząc audyt tego obszaru warto zwrócić uwagę, czy zachowana jest poufność danych przez wykorzystanie mechanizmów szyfrowania.

Plany zapewnienia ciągłości działania

Ustawa KSC[30] określa wymogi wdrożenia przez OUK odpowiednich i proporcjonalnych do szacowanego ryzyka środków technicznych i organizacyjnych zapewniających bezpieczeństwo i ciągłość dostaw usług, od których zależy świadczenie usługi kluczowej. W ramach realizacji tych zadań OUK powinien regularnie przeprowadzać analizę wpływu zdarzenia na biznes (*Business Impact Analysis* – BIA). Analiza BIA określa krytyczne procesy i zasoby niezbędne do realizacji usług kluczowych. Celem BIA jest nadanie priorytetów ryzyku, zarówno ilościowo, jak i jakościowo oraz wypracowanie planów radzenia sobie z zagrożeniami. W ramach analizy BIA określane są kluczowe wskaźniki dotyczące docelowego czasu odtworzenia procesu i zasobów (*Recovery Time Objective* – RTO i *Recovery Point Objective* – RPO), budowana jest też minimalna akceptowalna konfiguracja (MAK) dla procesów[31].

Przeprowadzając audyt tego obszaru warto zwrócić uwagę, czy w strukturach OUK znajduje się zespół, który zarządza i nadzoruje procesy ciągłości działania operatora. System zarządzania ciągłością jest ściśle powiązany z zarządzaniem kryzysowym. Kluczowa jest weryfikacja, czy dla dokumentacji bezpieczeństwa OUK przewidziano politykę zarządzania ciągłością oraz strategię BCM (*Business Continuity Management*). BCM powinna obejmować środki prewencyjne i ochronne, wskazywać potencjalną niedostępność systemów oraz kontrahentów i kluczowych dostawców. Warto przeanalizować szczegółowe procesy biznesowe, zasoby i podlegające im scenariusze niedostępności, które powinny być realizowane przez OUK w ramach analizy BIA. Ważne jest, aby analizę przeprowadzali właściciele procesów i zasobów. Metodyka BIA uwzględnia policzalne (np. finansowe) i jakościowe kategorie wpływu (np. skutki prawne, reputacja) niedostępności na procesy biznesowe. Ważne jest, aby krytyczne procesy operatora i ich rola były określone kompleksowo i aby prowadziło to do tworzenia planów ciągłości działania (*Business Continuity Planning* – BCP) i planu awaryjnego (*Distribution Requirements Planning* – DRP)[32]. Dobrą praktyką w zarządzaniu ciągłością działania jest wykorzystanie standardu ISO 22301[33].

Plany BCP i DRP powinny być dokumentami chronionymi. Plan zapewnienia ciągłości działania często jest dokumentem

[30] Art. 8.2. Ustawy z 5.7.2018 o Krajowym Systemie..., op.cit.
[31] K. Liderman: *Bezpieczeństwo informacyjne…*, op.cit., s. 239-240.
[32] K. Liderman: *Bezpieczeństwo informacyjne…*, op.cit., s. 241-262.
[33] *ISO 22301:2019 Security and resilience – Business continuity management systems – Requirements*, Genewa 2019 r.

niedocenianym przez kierownictwo OUK. Dopiero zewnętrzne okoliczności (wymogi regulacyjne, współpraca z zaawansowanym w tym obszarze partnerem, katastrofa lub sytuacja kryzysowa) prowadzą do opracowania dokumentów zapewnienia ciągłości procesów biznesowych.

Plan BCP składa się z fazy aktywacji, odtworzenia i przywrócenia[34]. Faza aktywacji obejmuje proces powiadomienia personelu odpowiedzialnego za odtworzenie procesu biznesowego i przeprowadzenie oceny szkody do chwili podjęcia decyzji do uruchomieniu planu. Faza odtworzenia koncentruje się na planach DRP. Faza przywrócenia skupia się na odtworzeniu operacyjnej funkcji operatora, zarówno w obiekcie istniejącym, jak i nowym. Plan BCP powinien zawierać listę kontaktów na potrzeby zarządzania kryzysowego, określać ich role i odpowiedzialność, sposoby i kanały komunikacji, procedury odtworzenia procesów biznesowych oraz scenariusze łagodzenia ryzyka.

Badając ten obszar warto zwrócić uwagę nie tylko czy analiza BIA jest regularnie przeprowadzana i daje wystarczające informacje do tworzenia planów BCP i DRP, ale również, czy plany są cyklicznie aktualizowane oraz testowane. Plany BCP szybko stają się nieaktualne (zmiana technologii, łączenie przedsiębiorstw, zmiany personalne). Warto więc zwrócić uwagę, czy zdefiniowano odpowiedzialność operatora za jego realizację, czy postanowienia zawarte w planach były zatwierdzane przez kierownictwo wyższego szczebla, czy kadra odpowiedzialna za przygotowywanie i aktualizację planów wykonuje te same zadania w ramach powierzonych jej obowiązków pracowniczych.

Podsumowanie

Audyt cyberbezpieczeństwa operatorów usług kluczowych w ramach ustawy KSC to swego rodzaju zdjęcie organizacji. Wskazuje miejsce, w którym podmiot się znajduje oraz kierunki rozwoju. Jest też ważnym elementem budowania bezpiecznego środowiska służącego zapewnieniu usług kluczowych. Jego wyniki nie tylko informują na ile organizacja jest gotowa do realizacji celów związanych z cyberbezpieczeństwem, ale również wskazują kierunki przyszłych działań. To ważne narzędzie dające wiedzę i pozycjonujące operatora w danym sektorze. Stosowanie metodycznego podejścia, uwzględniającego specyfikę branży, w której działa podmiot, zwiększa efektywność działań, skraca czas przeprowadzenia badania i ułatwia komunikację z jednostką kontrolowaną.

Zauważalna jest tendencja, że przepisy prawa nie definiują konkretnego sposobu tworzenia systemu cyberbezpieczeństwa, a raczej wskazują kluczowe obszary. Sztywne wymogi regulacyjne zastępowane są otwartością na własne, dobre metody wprowadzane przez OUK. Rolą audytora jest wspieranie tych działań, korygowanie tam gdzie jest to niezbędne oraz podkreślanie znaczenia, jeśli brakuje takiej świadomości wśród interesariuszy. Jego zadaniem nie jest utrudnianie realizacji

[34] K. Liderman: Bezpieczeństwo informacyjne…, op.cit., s. 242.

usługi kluczowej, ale pomoc w znalezieniu optymalnych i najbezpieczniejszych rozwiązań.

Być może w niedalekiej przyszłości audyt zastąpi technologia Blockchain, czyli system rejestru rozproszonego, który może być użyteczny wszędzie tam, gdzie występuje kontrola autentyczności, zgodności i nadzór regulacyjny. Do tego czasu audyt pozostanie najważniejszym narzędziem podejmowanym w ramach działań nadzorczych związanych z cyberbezpieczeństwem operatora usług kluczowych, służącym budowie systemu bezpieczeństwa narodowego.

ADAM WYGODNY
ekspert nadzoru
nad cyberbezpieczeństwem
w sektorze bankowym

Słowa kluczowe: krajowy system cyberbezpieczeństwa, ustawa KSC, audyt bezpieczeństwa systemu informacyjnego, audyt cyberbezpieczeństwa operatorów usług kluczowych, operator usługi kluczowej, metodyka audytu IT

Bibliografia

1. Axelos: *ITIL Foundation – v4*, TSO, 2019 r.
2. K. Bradley: *Podstawy metodyki Prince 2*, CRM, Warszawa 2002 r.
3. A. Chrysikos: *IT Security Audit, London Metropolitan University*, 2019 r.
4. *COBIT 5 – Metodyka biznesowa w zakresie nadzoru nad technologiami informatycznymi w przedsiębiorstwie i zarządzania nimi*, ISACA, 2012 r.
5. *Cybersecurity skills development in the EU*, ENISA, Greece 2020 r.
6. K. Czaplicki, A. Gryszczyńska, G. Szpor: *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, Wolters Kluwer Polska, Warszawa 2019 r.
7. W. Dańczyszyn: *Metodyki budowania programu cyberbezpieczeństwa*, materiały EY w ramach studiów podyplomowych SGH, Warszawa 2019 r.
8. C. Dotson: *Bezpieczeństwo w chmurze. Przewodnik po projektowaniu i wdrażaniu zabezpieczeń*, PWN, Warszawa 2020 r.
9. T. Herath, H. Herath, W. Bremser: *Balanced Scorecard Implementation of Security Strategies, Framework for IT Security Performance Management*, T&F, 2010 r.
10. *International Standard ISO/IEC 27001:2019, Information Technology – Security Techniques – Information Security Management Systems – Requirements*, Genewa 2019 r.
11. *ISO 22301:2019 Security and resilience – Business continuity management systems – Requirements*, Genewa 2019 r.
12. E. Jarzęcka-Siwik, B. Skwarka: *Komentarz do ustawy o NIK*, Difin, Warszawa 2017 r.
13. R. S. Kaplan, D. P. Horton: *Strategiczna Karta Wyników. Jak przełożyć strategię na działanie*, PWN, Warszawa 2001 r.

14. *Kompendium kontroli. Cyberbezpieczeństwo w UE i państwach członkowskich UE,* Unia Europejska, 2020 r.
15. KNF: *Komunikat KNF dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej*, Warszawa 2020 r.
16. KNF: *Rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach*, Warszawa 2013 r.
17. K. Liderman: *Bezpieczeństwo informacyjne. Nowe Wyzwania*, PWN, Warszawa 2017 r.
18. J. Molesky: *Lean Technology Strategy: Moving Fast With Defined Constraints,* LinkedIn Learning, 2018 r.
19. M. Niepłowicz: *Zrównoważona karta wyników dla departamentu audytu wewnętrznego*, WNEIZ, 2009 r.
20. Raport Polskiej Platformy Bezpieczeństwa Wewnętrznego: O*programowanie i narzędzia wspomagające analizę kryminalną*, Warszawa 2019 r.
21. Risk IT Practitioner Guide, USA, 2009 r.
22. M. Wrzosek: C*yberbezpieczeństwo A.D. 2019*, Warszawa, 2020 r.

ABSTRACT

Methods for Cybersecurity Auditing – Act on the National Cybersecurity System

The Act on the National Cybersecurity System (Polish: *Krajowy System Cyberbezpieczeństwa,* KSC), which is the first regulation that provides legal and organisational basis for a cybersecurity system, was signed by the President of Poland on 1 August 2018. The adoption of the Act is a response to the obligatory implementation of the Directive of the European Parliament and of the Council on security of network and information systems (the NIS Directive). The objective of the Act on KSC is to establish an effective information technology system at the national level. It defines the entities that constitute the system, especially key services operators, and obliges them to conduct regular audits of IT systems security. At the same time, the Act emphasises the importance of providing a method for unified reporting on audit results, in this way minimising subjectivity of evaluations – yet the Act itself does not define the method. The methodology for IT security auditing should combine, in a comprehensive manner, legal requirements and standards with good practices in the area. In his article, the author has attempted to summarise the methodologies and standards for cybersecurity management, taking into account the experience of auditors.

Adam Wygodny, expert in cybersecurity supervision in the banking sector

Key words: national cybersecurity system, Act on KSC, IT security audit, audit of key services operators cybersecurity, key services operators, IT audit methodology