Dr Łukasz Kister,
Ekspert [Cyber]Bezpieczeństwa - BezpieczneInformacje.PL

Audyt cyberbezpieczeństwa Usługi Kluczowej - czyli wiódł ślepy kulawego!

Wymagania Krajowego Systemu Cyberbezpieczeństwa

Operatorzy Usług Kluczowych zobowiązani są do prowadzenia audytów bezpieczeństwa Systemów Informacyjnych wykorzystywanych do ich świadczenia. Pierwszy z nich ma się odbyć po roku od otrzymania decyzji wyznaczającej, a kolejne w 2-letnich odstępach. Jak jednak przeprowadzić taki audyt - by miał on sens, a nie był tylko „sztuką dla sztuki", bo termin ucieka? Na to właśnie pytanie postaram się odpowiedzieć w tym artykule.

W ostatnich kilku miesiącach nastąpił wysyp różnego rodzaju zapytań i postępowań na wykonanie usługi tzw. audytu uKSC, ogłaszanych przez Operatorów Usług Kluczowych, którym wiosną kończy się termin 12 miesięcy od otrzymania decyzji administracyjnej właściwego organu ds. cyberbezpieczeństwa. Niestety nawet poważne i doświadczone grupy energetyczne nie wiedzą lub nie rozumieją: co chcą audytować, jak chcą audytować, po co chcą się audytować i przez kogą chcą być audytowani? Pozwólcie, że swoją ocenę tej sytuacji uprzejmie przemilczę.

Co mamy audytować?

Tak samo jak w pozostałych obowiązkach, tak również w zdefiniowaniu wymaganego „audytu", ustawodawca[1] nie wykazał się należytą i oczekiwaną starannością. Można nawet pokusić się o stwierdzenie, że określone zostało to, co nie ma praktycznie żadnego znaczenia dla przeprowadzenia badania audytowego. Generalnie, tak jak w poprzednio opisanych przypadkach, zupełnie mnie to nie dziwi, ale jednak za każdym razem trudno to pojąć, że coś co jest wymagane pod groźbą wysokiej kary finansowej, nie zostało zupełnie wyjaśnione (sic!).

Niemniej jednak, Operatorzy Usługi Kluczowej muszą się jednak zmierzyć z tym obowiązkiem, nie tyle by zaspokoić żądne wiedzy organy właściwe[2], ale przede wszystkim by pozyskać wiedzę o poziomie wdrożenia systemu zarządzania cyberbezpieczeństwem świadczonej Usługi Kluczowej. Dlatego tak ważne jest ustalenie podstawowych wyznaczników przygotowywanego audytu. By nie zostać jednak posądzonym o tworzenie własnych teorii, w tym artykule będę opierał się na wymaganiach dwóch uznanych międzynarodowych dokumentów:

- PN-EN ISO 19011 - Wytyczne dotyczące audytowania systemów zarządzania,
- Podręcznik kontroli systemów informatycznych dla najwyższych organów kontroli (WGITA-IDI).

Zacznijmy więc od próby zdefiniowania „zakresu audytu", tj. obszaru i granic audytu.

Operator Usługi Kluczowej ma obowiązek zapewnić przeprowadzenie, co

[1]Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, (Dz.U. poz. 1560, z późn. zm.).

[2]Jeden z nich - grożąc karami, wymusił przeprowadzenie audytu w okresie „stanu epidemii" i największych obostrzeń bezpieczeństwa sanitarnego.

najmniej raz na 2 lata, audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (art. 15 ust. 1 uKSC).

I to jest wszystko czego dowiadujemy się z Ustawy w przedmiocie formalnych wymagań względem audytu.

Czym jest „audyt bezpieczeństwa", czyli o kryteriach audytu napiszę w następnej części. Teraz skupmy się na próbie określenia obszaru fizycznego i logicznego wymaganych, a raczej merytorycznie uzasadnionych, czynności audytorskich.

Ustawowa definicja ograniczałaby audyt wyłącznie do pojedynczych Systemów Informacyjnych wykorzystywanych do świadczenia Usługi Kluczowej. Użycie przez ustawodawcę liczby pojedynczej jest tutaj bezdyskusyjne. Nie ma tutaj mowy ani o audytowaniu bezpieczeństwa świadczenia Usługi Kluczowej (sic!), ani o zbiorczym podejściu do współistniejących, a czasami nawet współzależnych Systemów Informacyjnych.

Jeżeli jednak mówimy o obowiązku stworzenia przez wyznaczony podmiot pewnego systemu cyberbezpieczeństwa świadczonej Usługi Kluczowej, to **audytem należy objąć:**

- całą Usługę Kluczową, ze szczególnym uwzględnieniem jej kontekstu,
- Systemy Informacyjne wykorzystywane do jej świadczenia[3], wraz z ich powiązaniami i współzależnościami,
- systemy wspierające niezakłócone funkcjonowanie samej Usługi Kluczowej, jak również poszczególnych Systemów Informacyjnych.

Taki zakres wynikać będzie również z wymaganych kryteriów audytu, o których dalej. Oczywiście otwarte pozostaje zagadnienie audytowania zewnętrznych systemów i usług wspierających, których niezakłócone działanie ma krytyczny wpływ na świadczoną Usługę Kluczową. Tutaj nie powinno być jednak dyskusji o tym czy powinniśmy to robić w świetle wymagań Ustawy, ale kiedy rozszerzyć plan audytu o takie czynności.

Jakie mają być kryteria audytu?

Wynik audytu jest uzależniony od zestawu wymagań jakie przyjmiemy za punkt odniesienia, dla którego będziemy zbierali dowody audytowe, a następnie dokonywali ich oceny. Tutaj sytuacja już może być nieco łatwiejsza do ustalenia, choć ustawodawca także w tym zakresie milczy w znany sobie sposób.

Osobiście zalecam przygotowanie tzw. **listy kontrolnej**, która pozwoli na inwentaryzację i agregację wszystkich wymagań, a następnie przypisanie im wyników audytu. Jak bardzo będzie ona szczegółowa, zależy tylko od nas. Należy jednak pamiętać, że jej precyzja będzie pomocna nie tylko w trakcie audytów.

Praktyka audytorska nakazuje, by znalazły się w niej takie pola informacyjne jak:

- kategoria wymagania: ustawa, rozporządzenie, norma,
- identyfikator wymagania: artykuł, paragraf, punkt,
- treść wymagania: ogólna (obszarowa) i szczegółowa.

Wymagania prawne należy wprost zaczerpnąć z:

- ustawy o krajowym systemie cyberbezpieczeństwa (art. 8-15),
- rozporządzenia w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo[4],
- rozporządzenia w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej[5].

Natomiast kryteria wynikające z obowiązku wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji zgodnego z normą PN-EN ISO/IEC 27001: Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Wymagania, to:

- wymagania części ogólnej normy (pkt. 4-10),
- wykaz celów stosowania zabezpieczeń (Załącznik A - Tablica A.1).

Ponadto, mając na uwadze dyspozycję art. 8 ust. 2 lit. c) i d) Ustawy, tj. obowiązki zapewnienia ciągłości niezakłóconego działania Usługi Kluczowej, zasadnym jest umieszczenie na liście kontrolnej także wymagań wynikających z normy PN-EN ISO 22301: Bezpieczeństwo powszechne - Systemy zarządzania ciągłością działania - Wymagania. Wdrożenie tej normy nie jest już obecnie obowiązkowe[6], ale obowiązkowe pozostaje posiadanie dokumentacji jej wdrożenia (sic!)[7].

Dodatkowo, szczególnie przez ustawodawcę nobilitowany proces zarządzania incydentami warto poddać weryfikacji w odniesieniu do zasad określonych w normie EN ISO/IEC 27035: Technologia informacyjna - Techniki bezpieczeństwa - Zarządzanie incydentami związanymi z bezpieczeństwem informacji.

[3] O identyfikacji Systemów Informacyjnych pisałem w numerze 3 (68)/2019 „Nowa Energia".

[4] (Dz.U. 2019, poz. 2479).

[5] (Dz.U. 2018, poz. 2080).

[6] Patrz: uchylone rozporządzenie ws. warunków organizacyjnych i technicznych (Dz.U. 2018, poz. 1780).

[7] Patrz: §2 pkt 3.

Tak stworzona lista kontrolna to ok. **200 wymagań**, które oczywiście mogą się częściowo pokrywać i uzupełniać, ale ich weryfikacja daje rzeczywisty obraz systemu zarządzania cyberbezpieczeństwem Usługi Kluczowej.

Jaka metodologia badań audytorskich?

Mając na uwadze cel, zakres i kryteria audytu należy jednoznacznie wskazać, że najskuteczniejszym i najsprawniejszym sposobem zebrania obiektywnych dowodów potwierdzających wypełnianie wymagań prawnych i normatywnych, będzie **klasyczny audyt**, oparty na:

- analizie dokumentacji odnoszącej się do samej Usługi Kluczowej oraz Systemów Informacyjnych,
- wywiadach z osobami zaangażowanymi w proces utrzymania Usługi Kluczowej oraz Systemów Informacyjnych,
- obserwacja procesów związanych z funkcjonowaniem Usługi Kluczowej oraz Systemów Informacyjnych, ze szczególnym zwróceniem uwagi na procedury reagowania kryzysowego.

Audyt powinien być przeprowadzany fizycznie w miejscu funkcjonowania Systemów Informacyjnych, ale jego wybrane elementy mogą być wykonywane w formie zdalnej, przy zachowaniu niezbędnych standardów ochrony informacji.

Niemniej jednak należy pamiętać o istocie audytu, która nie opiera się o szczegółowe badanie wszystkich procesów i ich składowych, ale o właściwe dobieranie takich wielkości i jakości **próbek**, które dadzą możliwość oceny całości. Możemy tutaj zastosować zarówno model pobierania próbek w oparciu o osąd i doświadczenie eksperckie audytorów, jak również wynikające z kryterium statystycznego rozkładu danej populacji.

Kończąc ten wątek, chciałbym odnieść się do nieuprawnionych opinii, że przedmiotowy audyt musi opierać się na fizycznym testowaniu Systemów Informacyjnych i ich bezpieczeństwa, np. testy penetracyjne. Po pierwsze, nigdzie w Ustawie nie znajdziemy takiego obowiązku, choćby domyślnego. Po drugie, audyt systemu zarządzania, a takie jest tutaj wymaganie, ocenia wdrożenie i sam nie powinien być uwikłany w działania ocenne, np. czy można było przeprowadzić inaczej lub innymi narzędziami test penetracyjny. Po trzecie, jednym z celów audytu jest weryfikacja, czy organizacja właściwie zarządza bezpieczeństwem Systemu Informacyjnego, czy zbiera i weryfikuje informacje o podatnościach.

Co ma zawierać raport z audytu?

Skoro ustawodawca niczego nie doprecyzował, to trudno oczekiwać by inaczej było w przypadku wymagań od formalnego efektu audytu. Jedyne co wiemy to to, że raport:

- ma powstać na podstawie *„zebranych dokumentów i dowodów”* - trudno, żeby powstał na podstawie marzeń i oczekiwań (sic!),
- ma zostać sporządzony w formie „pisemnego sprawozdania” - czy to oznacza, że nie może być w formie elektronicznej?,
- ma zawierać „dokumentację z przeprowadzonego audytu” - taką dokumentacją przekazywaną audytowanemu jest raport, a więc o co tutaj może chodzić - o notatki audytorów, wydruki, kopie dokumentów?,
- ma zostać przekazany Operatorowi Usługi Kluczowej (art. 15 ust. 5 uKSC).

Co ciekawe, również rozporządzenie ws. obowiązkowej dokumentacji cyberbezpieczeństwa[8] zupełnie pomija wymaganie w zakresie udokumentowania audytu Systemu Informacyjnego wykorzystywanego do świadczenia Usługi Kluczowej. Z drugiej zaś strony, udokumentowanie audytów jest jednym z kluczowych obowiązków w wymaganych od Operatora Usługi Kluczowej systemach zarządzania - ISO 27001 oraz ISO 22301.

Na próżno też szukać w tym zakresie zaleceń Ministerstwa Cyfryzacji, CSIRT'ów poziomu krajowego, czy organów właściwych ds. cyberbezpieczeństwa.

Skoro tak, to wracamy do uznanego międzynarodowego standardu dotyczącego audytowania, a więc wspominanej wcześniej normy ISO 19011. Moim zdaniem, szukanie na siłę autorskich pomysłów jest mocno nietrafione i kontrproduktywne. Szczególnie z uwagi na i tak obowiązkowe audytowanie wdrożonych systemów ISO 27001 i ISO 22301, które musi opierać się na wskazanej normie. Oczywiście im więcej różnych audytów - w granicach rozsądku, tym więcej szans na wykrycie niezgodności i ich skorygowanie.

Raport z audytu można generalnie podzielić na trzy główne części:

- wnioski audytorskie,
- informacje formalno-organizacyjne,
- ustalenia audytowe i potwierdzające je dowody.

Wnioski muszą otwierać raport z audytu - oczywiście pomijam kwestie strony tytułowej. Po ich przeczytaniu kierownictwo Operatora Usługi Kluczowej musi mieć wiedzę, czy i na jakim poziomie spełnione zostały wymagania stawiane przez Ustawę i rozporządzenia wykonawcze. Poza generalnym wnioskiem zgodności lub braku zgodności z kryteriami audytu, należy umieścić tutaj także odniesienie do zidentyfikowanych obszarów wymagających doskonalenia.

Wnioski nie mogą być jednak tylko zbiorem wytyków. Tym samym, dobrą praktyką jest również informowanie w

[8]Rozporządzenie Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (Dz.U. poz. 2080).

tym miejscu o zauważonych sukcesach, dobrych praktykach, czy szczególnym zaangażowaniu. Audyt to nie kontrola w administracji. Tutaj równie ważne jest pokazywanie spełnienia wymagań, jak i działań wymagających naprawy.

Część formalno-organizacyjna raportu wcale nie jest taka zupełnie pozbawiona walorów merytorycznej wartości dla czytelnika. To w niej znajdujemy wszystkie informacje identyfikujące czas, sposób i formę przeprowadzenia audytu, a tym samym elementy mające decydujący wpływ na jego przebieg i wnioskowanie.

W tej części należy bezwzględnie pamiętać o umieszczeniu informacji o:

- dacie audytu - od pierwszej do ostatniej czynności,
- audytowanym podmiocie lub podmiotach,
- audytowanych Systemach Informacyjnych,
- miejscach prowadzenia audytu,
- celu audytu,
- zakresie audytu,
- kryteriach audytu,
- podstawach prawnych i formalnych przeprowadzenia audytu,
- zespole audytorskim,
- przedstawicielach audytowanego, którzy brali udział w czynnościach,
- uwagach i zastrzeżeniach do przebiegu czynności audytorskich,
- nierozstrzygniętych wątpliwościach i ich przyczynach,
- poufnym charakterze treści raportu.

Najobszerniejszą częścią raportu są **ustalenia audytowe**, które muszą być wiernym i potwierdzonym dowodami obrazem rzeczywistości Systemów Informacyjnych, w odniesieniu do przyjętych kryteriów audytu. W naszym przypadku będą to wymagania określone w Ustawie, rozporządzeniach wykonawczych oraz - a może przede wszystkim - międzynarodowych normach ISO 27001 i 22301.

Praktyka audytorska pokazuje, że najlepszym modelem przedstawiania ustaleń audytowych jest wskazywanie kolejno po sobie:

- identyfikacji wymagania - artykuł ustawy, paragraf rozporządzenia lub punkt normy,
- krótki opis wymagania,
- stopień spełnienia wymagania - zgodność / doskonalenie / niezgodność,
- opis stanu rzeczywistego i związanych z nim dowodów[9].

Dodatkowo do każdego z wymagań, dla których stwierdzono niezgodności lub możliwości doskonalenia, należy odnotować uzgodnione pomiędzy audytorami, a audytowanymi, warunki działań korekcyjnych i korygujących.

Podsumowując: jaki ma być więc raport z audytu? Najlepiej: krótki, zwięzły, konkretny, precyzyjny, a przede wszystkim - zrozumiały dla kierownictwa Operatora Usługi Kluczowej, a nie dla jego informatyków.

Jakich audytorów wybrać? - zamiast zakończenia

Czy decydując się na powierzenie podmiotowi zewnętrznemu przeprowadzenia audytu wystarczy, że wskażemy wymagania Ustawy (art. 15 ust. 2) oraz obowiązek posiadania certyfikatów wskazanych w rozporządzeniu[10]? Odpowiedź brzmi: oczywiście, że nie! Nie traktujmy tego audytu jak kolejnego wymogu prawnego, do zrealizowania na tzw. „sztukę", ale jako źródło rzetelnej wiedzy o naszej organizacji i jej bezpieczeństwie.

Audyt to umiejętność potwierdzania deklaracji i zbierania dowodów, a nie pasjonowanie się takim, czy innym obszarem bezpieczeństwa IT. Stąd audytor nie musi być ekspertem od tej czy innej technologii, bo wtedy skupi się tylko na swoim „koniku", ale doświadczonym analitykiem, potrafiącym korelować informacje i ustalać stan rzeczywisty, w oparciu o fakty, a nie własne chciejstwo, czy też uprzedzenia.

Ponadto pamiętajmy, że wpuszczając audytora do swojej organizacji, otwieramy przed nim wszystkie „szafy z tajemnicami". Nie wybierajmy „kryterium ceny", a świadomie szacujmy ryzyko. □

Dr Łukasz Kister
Doktor nauk o bezpieczeństwie. Biegły sądowy przy Sądzie Okręgowym w Warszawie.
Audytor Wiodący Systemu Zarządzania Bezpieczeństwem Informacji - ISO 27001 oraz Systemu Zarządzania Ciągłością Działania - ISO 22301, Risk Manager - ISO 31000 / 27005, Incident Response Manager - ISO 27035.
20 lat praktycznych doświadczeń w projektowaniu, wdrażaniu i audytowaniu systemów bezpieczeństwa w instytucjach publicznych i biznesie. Stworzył Departament Bezpieczeństwa Polskich Sieci Elektroenergetycznych S.A., zbudował i doprowadził do akredytacji Zespół Reagowania na Incydenty Komputerowe - CERT PSE, a spółkę wprowadził do Centrum Eksperckiego Bezpieczeństwa Energetycznego NATO (EnSec CoE). Zainicjował powstanie i kierował Zespołem ds. Cyberbezpieczeństwa Polskiego Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej (PTPiREE). Był polskim przedstawicielem w Grupie Roboczej ds. Ochrony Systemów Krytycznych Europejskiego Zrzeszenia Operatorów Przesyłowych Energii Elektrycznej (ENTSO-e). Dumny posiadacz tytułu „Ambasador Polskiej Gospodarki".

[9]Brak wskazania dowodów - o charakterze obiektywnym, potwierdzających ustalenia audytowe, dyskwalifikuje cały audyt.
[10](Dz.U. 2018, poz. 1999).