CERTYFIKACJA PRODUKTÓW I USŁUG TELEINFORMATYCZNYCH Z UWZGLĘDNIENIEM POTRZEB SEKTORA BANKOWEGO

DR INŻ. ELŻBIETA ANDRUKIEWICZ

SYGN. WIB PAB 2020/1

Raport opracowany na zlecenie Programu Analityczno-Badawczego
Fundacji Warszawski Instytut Bankowości

Warszawa, 15.01.2020

PROGRAM ANALITYCZNO BADAWCZY

O Raporcie

Raport **Certyfikacja produktów i usług teleinformatycznych z uwzględnieniem potrzeb sektora bankowego** został opracowany na zlecenie Programu Analityczno-Badawczego Fundacji Warszawski Instytut Bankowości

Autorzy:

dr inż. Elżbieta Andrukiewicz
Kierownictwo merytoryczne

Doktor nauk technicznych, absolwentka Wydziału Elektroniki Politechniki Warszawskiej. Wybitny ekspert polski i międzynarodowy w obszarze zarządzania bezpieczeństwem informacji, architektury bezpieczeństwa, ewaluacji cyberbezpieczeństwa. Jest autorką licznych publikacji oraz prezenterem i wykładowcą na konferencjach i warsztatach poświęconych tematyce cyberbezpieczeństwa w Polsce i na świecie. Audytor wiodący systemów zarządzania bezpieczeństwem informacji, z wieloletnim doświadczeniem praktycznym zdobytym w trakcie ponad 100 audytów bezpieczeństwa teleinformatycznego, w tym również w sektorze bankowym. Edytor norm międzynarodowych i europejskich z zakresu bezpieczeństwa informacji i ewaluacji cyberbezpieczeństwa. Ekspert ENISA od 2017 roku, jest autorem opracowań i ekspertyz w obszarze cyberbezpieczeństwa.

PROGRAM ANALITYCZNO BADAWCZY

O Programie

Program Analityczno-Badawczy przy Fundacji Warszawski Instytut Bankowości powstał w 2019 roku jako odpowiedź na potrzeby sektora bankowego w zakresie wysokiej jakości analiz i badań z obszaru cyberbezpieczeństwa i nowych technologii, a także szeroko rozumianego otoczenia sektora bankowego, kształtującego warunki działania banków w Polsce.

Prace analityczno-badawcze w ramach programu realizowane są pod kątem możliwości praktycznego wykorzystania wyników w celu rozwoju sektora bankowego, podnoszenia poziomu bezpieczeństwa usług oraz – w ostateczności – kreowania wartości dla klientów – końcowych użytkowników bankowości.

W ramach programu realizowane są analizy i badania w następujących obszarach:

- **Nowe technologie i cyberbezpieczeństwo**
- **Zdolność banków do finansowania gospodarki**
- **Bankowość spółdzielcza**
- **Rynek nieruchomości**
- **Zielony ład i finansowanie energetyki odnawialnej**
- **Finansowanie projektów innowacyjnych**

Więcej na temat działalności programu na stronie www.pab.wib.org.pl

Kontakt:

dr Andrzej Banasiak
Koordynator Programu
m: 696 405 104
e: abanasiak@wib.org.pl

Jacek Gieorgica
m: 603 626 254
e: jgieorgica@wib.org.pl

Warszawski Instytut Bankowości
00-394 Warszawa, ul. Solec 38, lok. 104
t: (22) 182 31 70
e: pab@wib.org.pl

Agnieszka Nierodka
m: 607 484 391
e: anierodka@wib.org.pl

dr Tomasz Pawlonka
m: 505 917 778
e: tpawlonka@wib.org.pl

Spis treści

Słowa kluczowe
Certyfikacja; cyberbezpieczeństwo; sektor bankowy; regulacje; Akt o Cyberbezpieczeństwie; Wspólny Rynek Cyfrowy; Dyrektywa NIS; rozwiązania chmurowe; cloud computing; Big Data; sztuczna inteligencja w sektorze bankowym; bezpieczeństwo teleinformatyczne; operator usługi kluczowej;standaryzacja; ład bezpieczeństwa; jakość procesów; jakość produktów; jakość usług; ochrona banku.

Streszczenie kierownicze

Cyberbezpieczeństwo stało się w ostatnich latach centralnym zagadnieniem w wielu sektorach gospodarki, w tym bankowym. Wraz z rozwojem technologicznym, w tym zwiększeniem znaczenia usług mobilnych, zmienia się krajobraz zagrożeń dla cyberbezpieczeństwa. Ogólnie można powiedzieć, że **cyberbezpieczeństwo** to wszystkie działania i mechanizmy wdrożone, by chronić system teleinformatyczny przed atakami, które mogłyby zagrozić poufności, integralności lub dostępności danych. W ramach cyberbezpieczeństwa mieszczą się metody prewencji ataku, wykrywania i reagowania na incydent bezpieczeństwa oraz odtworzenia funkcjonalności systemu po ataku.

Certyfikacja cyberbezpieczeństwa to potwierdzenie zgodności rozwiązań z określonymi kryteriami, dokonane przez niezależny podmiot na podstawie ewaluacji przeprowadzonej przez akredytowane laboratorium. W niektórych sektorach, np. technologii informacyjnych, certyfikacja jest szeroko rozpowszechniona i stanowi przewagę konkurencyjną firmy. W sektorze bankowym certyfikacja cyberbezpieczeństwa nie jest powszechna, lecz można prognozować, że to się zmieni w związku z polityką UE promocji Wspólnego Rynku Cyfrowego.

Działania UE, istotne dla sektora bankowego w kontekście cyberbezpieczeństwa, postępują dwutorowo. Pierwszy tor wyznacza **dyrektywa NIS**, wprowadzona w Polsce ustawą o Krajowym Systemie Cyberbezpieczeństwa. Banki, jako operatorzy usług kluczowych, stają się elementem ogólnoeuropejskiego systemu zgłaszania i reagowania na incydenty cyberbezpieczeństwa. Wśród najważniejszych wymogów stawianych operatorom usług kluczowych, należy wymienić obowiązek zapewnienia funkcjonowania zespołu reagowania działającego w trybie ciągłym oraz punktu kontaktowego dla krajowych zespołów reagowania na incydenty (CSIRT), które są wskazane w Ustawie.
Zakres podmiotowy i przedmiotowy usług kluczowych będzie z pewnością przedmiotem dalszego zainteresowania regulacyjnego UE. Zgodnie z zapowiedziami Komisji Europejskiej, w 2020 roku należy spodziewać się przeglądu dyrektywy NIS i dalszych prac, które mogą podnieść wymogi dotyczące systemów ochrony cyberprzestrzeni.
Istotnym kierunkiem rozwoju usług w cyberprzestrzeni będą w najbliższym czasie wdrożenia rozwiązań chmurowych, przy uwzględnieniu wymagań bezpieczeństwa wynikających z Rozporządzenia 2018/1807[1] dot. swobodnego przepływ danych nieosobowych w ramach UE. Jednocześnie w dalszym ciągu istotne wątpliwości i obawy natury prawnej (RODO) budzą rozwiązania chmurowe zapewniające przetwarzanie danych osobowych.

Drugim, komplementarnym torem podąża **Akt o Cyberbezpieczeństwie**, rozporządzenie unijne wprowadzające ogólnoeuropejskie ramy certyfikacji cyberbezpieczeństwa usług, produktów i procesów ICT. W wielu obszarach rozdrobnioną certyfikację krajową zastąpi jeden, europejski certyfikat bezpieczeństwa, który z pewnością będzie znacznie lepiej i powszechniej odbieraną gwarancją zgodności z wymogami bezpieczeństwa. Jednym z pierwszych obszarów wdrożenia Aktu o cyberbezpieczeństwie są rozwiązania chmurowe. Obecnie outsourcing usług, takich jak chmura, jest w sektorze bankowym ściśle regulowany, jednak rozpowszechnienie jednolitej certyfikacji może wpłynąć na zmianę tego stanu.

W toku prac nad Aktem o Cyberbezpieczeństwie pojawił się pomysł **obowiązkowej certyfikacji cyberbezpieczeństwa**. Choć w końcowym efekcie pozostała koncepcja dobrowolności, to należy przyjąć, że obowiązek certyfikacji cyberbezpieczeństwa w obszarze usług kluczowych pojawi się w bliskiej przyszłości, w perspektywie 2-3 lat.

Akt o Cyberbezpieczeństwie wprowadza zatem kontekst regulacyjny dla certyfikowanych produktów i usług stosowanych w sektorze płatniczym (będących usługami kluczowymi). Jednocześnie, rynek certyfikacji jest zdominowany przez organizacje globalne tzn. EMVCo i PCI, stworzone przez prywatne podmioty będące operatorami płatności i jako takie wydają certyfikaty, które są poza zakresem

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej.

stosowania Aktu o Cyberbezpieczeństwie. Należy zatem spodziewać się znacznych zmian w sektorze płatniczym przy rosnącej roli certyfikacji produktów i usług, a kierunek i siła tych zmian na pewno w najbliższym czasie będą przedmiotem dyskusji i kolejnych regulacji.

Certyfikacja cyberbezpieczeństwa nie jest obecnie istotnym czynnikiem marketingu banków, kierowanego do klientów indywidualnych i biznesowych. Jednak – jak wskazują wszystkie dostępne badania – świadomość zagrożeń cyberbezpieczeństwa, przede wszystkim związana ze wzrostem znaczenia bankowości internetowej i mobilnej, rośnie. Efekt braku zgłębienia kwestii certyfikacji bezpieczeństwa może wpłynąć w przyszłości negatywnie na opinię klientów o banku.

W kontekście znaczenia certyfikacji cyberbezpieczeństwa dla sektora bankowego, warto wspomnieć również o **dyrektywie PSD2**, wprowadzającej dla banków obowiązek udostępniania danych niezależnym usługodawcom, Third Party Providers (TPP). Punkt styku pomiędzy systemem banku a zewnętrznym usługodawcą tworzy kolejny obszar, który należy chronić przed atakami hakerów. Certyfikacja platform i interfejsów, wykorzystywanych na połączeniach systemów, będzie potwierdzeniem bezpieczeństwa stosowanych rozwiązań.

Polityka Wspólnego Rynku Cyfrowego UE silnie promuje **rozwiązania chmurowe**, zatem jednym z pierwszych obszarów objętych ogólnoeuropejską certyfikacją ma być właśnie chmura. Obecnie certyfikacja rozwiązań chmurowych jest rozproszona i rozwijana w krajach członkowskich niezależnie. Wprowadzenie unijnej certyfikacji cyberbezpieczeństwa spowoduje wzrost zaufania do rozwiązań chmurowych, co może pozytywnie wpłynąć na uelastycznienie podejścia KNF do outsourcingu.

Wstęp

Cyberbezpieczeństwo stało się w ostatnich latach centralnym zagadnieniem w wielu sektorach gospodarki, w tym bankowym. Zarówno w kontaktach z partnerami biznesowymi, jak i z klientami, kwestia bezpieczeństwa danych jest istotnym czynnikiem wzajemnego zaufania. Wraz z rozwojem technologicznym, w tym zwiększeniem znaczenia usług mobilnych, zmienia się krajobraz zagrożeń dla cyberbezpieczeństwa.

Nowe produkty i usługi online – czy to streaming mediów, zakupy on-line, media społecznościowe czy bankowość mobilna – stają się codziennością. Jednakże z każdą nowinką technologiczną niezbędną w naszym życiu, rośnie zagrożenie cyberatakami ze strony cyberprzestępców. Wraz z rozwojem Internetu Rzeczy, Big Data czy rozwiązań chmurowych, zwiększa się również liczba urządzeń narażonych na ataki.

Powszechna i nieznająca granic natura Internetu sprawia, że atak może nastąpić w kilku krajach jednocześnie, a jego skutki odczuwane są czasem po drugiej stronie globu. Co za tym idzie, zarówno dochodzenia, jak i próby pociągnięcia do odpowiedzialności przestępców muszą być ponadnarodowe.

Jest kilka najpopularniejszych typów ataków, których można stać się ofiarą jako użytkownik Internetu. **Malware** (malicious software) – złośliwe oprogramowanie, którego celem jest uszkodzenie urządzenia lub sieci. Typami malware'u są wirusy, trojany, adware czy spyware. **Ransomware** to program, który szyfruje dane, uniemożliwiając użytkownikowi dostęp do nich. Przywrócenie dostępu jest uzależnione od zapłaty okupu bądź wykonania żądanej akcji. **Distributed Denial of Service** (DDoS) polega na ataku na sieć poprzez wysłanie przez boty większej ilości zapytań, niż sieć jest w stanie przetworzyć. Innym typem cyberataków jest nakłanianie użytkownika do wykonania czynności, która mu zaszkodzi. Przykładem jest **phishing**, czyli mail podszywający się pod zaufane źródło proszący użytkownika np. o podanie informacji czy kliknięcie linka.

W sektorze płatności powszechnie znanym atakiem jest oszustwo **Card Not Present** (CNP). Wiele transakcji internetowych wymaga wprowadzenia, a co za tym idzie przechowywania podstawowych danych klienta (Primary Account Numbers PAN). Oszustwo Card Not Present polega na próbie wykorzystanie danych cudzej karty. Dane mogą być przejęte poprzez phishing czy wyciek danych ze sklepu internetowego. Jednym ze sposobów na obniżenie prawdopodobieństwa oszustwa jest np. prośba o kod CVV, który fizycznie znajduje się na drugiej stronie kart, przy każdej transakcji.

Z innych oszustw można wymienić **skimming**, polegający na skopiowaniu danych karty oraz **jackpotting**, typ malware'u atakujący oprogramowanie bankomatów, powodujący wypłatę całej składowanej gotówki.

Wg raportu Europolu, w 2019 roku najczęstszym typem ataku w Internecie był ransomware. Mimo że ogólna liczba takich ataków spadła, stały się one bardziej kosztowne dla zaatakowanego. Najczęstszym celem ataku są dane. Wśród oszustw finansowych najczęstszym typem jest oszustwo CNP, następnie skimming i jackpotting.

Od 2017 roku jednym z priorytetów Unii Europejskiej jest wzmocnienie bezpieczeństwa konsumenta w sieci, czy to poprzez silną ochronę danych osobowych (GDPR), czy przez zwiększanie wymogów bezpieczeństwa stawianych producentom i usługodawcom. Należy zauważyć, że kraje członkowskie UE, w tym Polska, mają wpływ na kształt regulacji unijnych podczas prac nad treścią regulacji, jednakże po ich przyjęciu obowiązkiem każdego kraju należącego do UE jest ich wdrożenie do prawa krajowego (dyrektywy NIS) albo bezpośrednie stosowanie (rozporządzenia lub akty delegowane). Także ogólnoeuropejskie organizacje doradcze oraz instytucje działające w sektorze bankowym, w tym również w ramach nadzoru bankowego, takie jak European Banking Authority, uczestniczą w procesie konsultacji przed wprowadzeniem regulacji.

Certyfikacja bezpieczeństwa produktów i usług teleinformatycznych wychodzi naprzeciw potrzebie potwierdzenia zaufania do stosowanych rozwiązań. Certyfikat dla danego produktu czy usługi daje uzasadnioną pewność, że zgodność założonej funkcjonalności bezpieczeństwa dla danego przedmiotu z wymaganiami została sprawdzona w rygorystyczny i ustrukturyzowany sposób.

Certyfikacja cyberbezpieczeństwa nie jest obecnie istotnym czynnikiem marketingu banków, kierowanego do klientów indywidualnych i biznesowych. Inaczej niż np. w branży IT, nie jest łatwo znaleźć na stronach internetowych informacje o posiadanych certyfikatach (patrząc z punktu widzenia konsumentów). Jednak – jak wskazują wszystkie dostępne badania – świadomość zagrożeń cyberbezpieczeństwa, przede wszystkim związana ze wzrostem znaczenia bankowości internetowej i mobilnej rośnie. Certyfikacja może stanowić odpowiedź na wątpliwości konsumentów w tym obszarze. Jest ona też jasnym i obiektywnym poświadczeniem sprawdzenia bezpieczeństwa produktu lub usługi.

Rozwiązania chmurowe cieszą się coraz większą popularnością, jednak wciąż stosuje je mniejszość firm. Sposobem na przezwyciężenie wątpliwości

użytkowników związanych z bezpieczeństwem danych i zwiększenie poziomu akceptacji rozwiązań chmurowych może być certyfikacja cyberbezpieczeństwa. Istniejące rozwiązania certyfikacyjne charakteryzują się znacznym rozproszeniem, zarówno na poziomie globalnym, jak i krajowym oraz niejasnością w odniesieniu do stosowanych norm referencyjnych do oceny zgodności. Dodatkowo wiele krajów wypracowało własne rozwiązania, których przestrzegania wymaga od chmur obliczeniowych działających na ich terytorium. Stąd jednym z pierwszych obszarów, które obejmie certyfikacja wprowadzona przez Akt o Cyberbezpieczeństwie, są rozwiązania chmurowe.

W sektorze bankowym chmura to bardzo obiecujące rozwiązanie. Przykładowo, korzystanie z mocy obliczeniowej do wprowadzania usług opartych na sztucznej inteligencji to jeden z bardziej interesujących kierunków rozwoju. Obecnie wykorzystanie chmury w działalności bankowej wymaga odrębnej zgody Komisji Nadzoru Finansowego, która konserwatywnie podchodzi do jakiegokolwiek outsourcingu, w tym z wykorzystaniem chmury. Wprowadzenie obowiązku certyfikacji, połączone z presją UE dotyczącą Wspólnego Rynku Cyfrowego, może zmienić podejście regulatora i szerzej otworzyć drzwi do wykorzystywania rozwiązań chmurowych.

System oceny zgodności

2.1. Ogólne pojęcie i specyfika oceny zgodności w cyberbezpieczeństwie

Ocena zgodności (ang. conformity assessment) jest terminem zdefiniowanym w normie ISO/IEC 17000 jako „wykazanie, że określone wymagania odnoszące się do produktów, procesów, systemów lub osób są spełnione". Podstawowymi procesami oceny zgodności są ewaluacja i certyfikacja.

Ewaluacja to: „oszacowanie przedmiotu oceny w odniesieniu do zdefiniowanych kryteriów" [ISO/IEC 15408-1], natomiast **certyfikacja** definiowana jest wg ISO/IEC 17000 jako „poświadczenie strony trzeciej w odniesieniu do produktów, procesów, systemów lub osób". W zależności od sektora, certyfikacja może być obowiązkowa, np. w odniesieniu do bezpieczeństwa żywności, lub dobrowolna np. w odniesieniu do systemów zarządzania bezpieczeństwem informacji.

Charakterystyczną cechą certyfikacji jest zatem poprzedzająca ją ewaluacja zgodności z określonym zbiorem wymagań. Aby ocena zgodności miała walor porównywalności dla różnych kategorii przedmiotów oceny, musi być przeprowadzona w odniesieniu do tego samego zbioru wymagań (specyfikacji technicznych). Stąd pojawia się rola norm międzynarodowych oraz standardów branżowych.

Specyficzna dla oceny zgodności w cyberbezpieczeństwie jest koncepcja **„poziomów uzasadnienia zaufania"** (assurance levels). „Poziom uzasadnienia zaufania" oznacza podstawę dla pewności, że dany produkt ICT, dana usługa ICT lub dany proces ICT spełnia wymogi bezpieczeństwa. Poziom uzasadnienia zaufania nie daje odpowiedzi na pytanie, czy produkt lub usługa lub proces jest bezpieczny, ale oznacza potwierdzenie, że z odpowiednią wnikliwością i rygorem badania sprawdzono, że produkt lub usługa spełnia spójne i kompletne funkcjonalne wymagania bezpieczeństwa.

2.2. Normy referencyjne

Normy referencyjne są podstawą ewaluacji, której potrzeba może wynikać z wymagań prawnych lub schematów certyfikacji. Przykładem normy referencyjnej jest ISO/IEC 27001. Norma referencyjna przywoływana jest w aktach prawnych, np. polskich czy unijnych. W kontekście schematu certyfikacji pojęcie normy referencyjnej może odnosić się też do standardów branżowych.

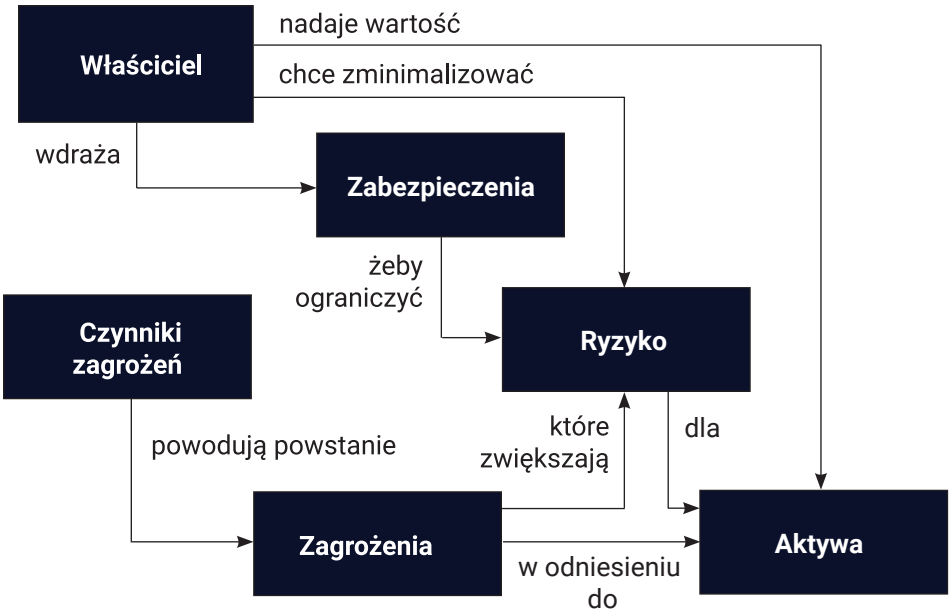
2.3. Normy zharmonizowane

Normy zharmonizowane są specjalną kategorią norm funkcjonujących w Europejskim Obszarze Gospodarczym, wspierających systemy oceny zgodności zdefiniowane w Rozporządzeniu 765/2008, dotyczącym nadzoru nad rynkiem. Normy te są opracowywane w europejskich jednostkach normalizacyjnych (CEN, CENELEC, ETSI) na podstawie mandatu udzielonego przez Komisję Europejską. Mogą być też przyjmowanymi normami międzynarodowymi. Normy zharmonizowane są publikowane w Dzienniku Urzędowym Unii Europejskiej i stanowią element prawodawstwa UE. Mają one numerację EN 170xx. Na podstawie wymagań zawartych w tych normach jednostki oceniające zgodność *(CAB – conformity assessment body)* otrzymują akredytację w różnym zakresie swoich kompetencji (np. certyfikacji wyrobów, procesów czy ludzi, prowadzenia badań, wzorcowania przyrządów czy porównań międzylaboratoryjnych).

2.4. Normy międzynarodowe jako normy referencyjne w schematach certyfikacji

Jest niewiele powszechnie uznawanych specyfikacji technicznych, czy to w postaci norm międzynarodowych, czy standardów sektorowych (branżowych) funkcjonujących jako standardy de facto, które mogą być podstawą ocen zgodności skutkujących powszechnie uznawanymi certyfikatami cyberbezpieczeństwa.

Podstawową normą dla oceny zgodności w dziedzinie bezpieczeństwa informacji jest norma **PN-EN ISO/IEC 27001**. Norma „określa wymagania dotyczące ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji w odniesieniu do organizacji" [ISO 27001]. W normie określone są także wymagania dotyczące zarządzania ryzykiem w bezpieczeństwie informacji. Jest to norma wykorzystywana w każdym sektorze, w którym gromadzi się i przetwarza dane, czyli właściwie wszędzie. Od kilkunastu lat istnieje możliwość certyfikacji systemów zarządzania bezpieczeństwem informacji na zgodność z normą ISO/IEC 27001. Jest to system o zasięgu globalnym, a certyfikaty zgodności wydane przez akredytowane jednostki certyfikujące są powszechnie uznawane. Więcej informacji o normie można znaleźć w załączniku A.



Rysunek 1. Model bezpieczeństwa zgodny z Common Criteria
Źródło: EN-ISO/IEC 15408-1

2.5. Common Criteria jako podstawa oceny ewaluacji bezpieczeństwa produktów IT

2.5.1. Wprowadzenie do Common Criteria

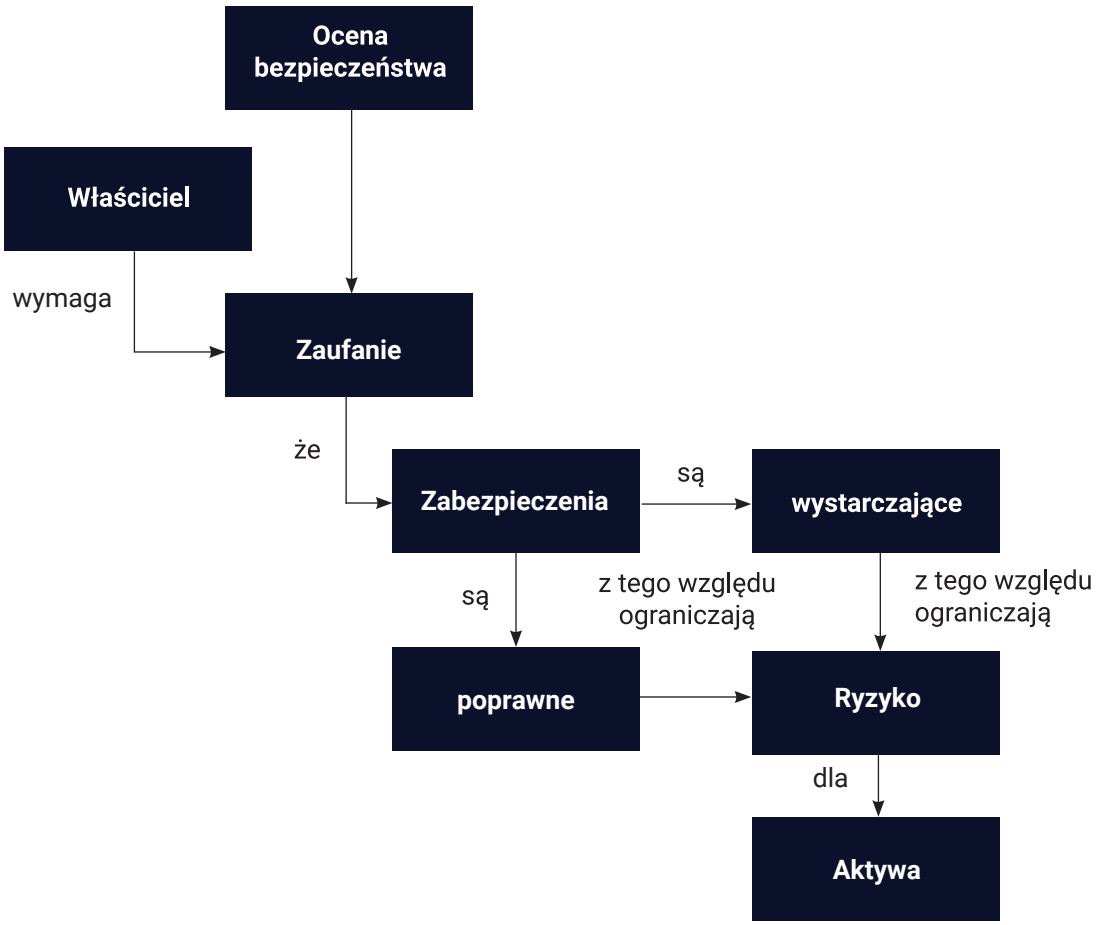
3-częściowa **norma ISO/IEC 15408**, będąca również polską normą PN-ISO/IEC 15408 „Kryteria oceny zabezpieczeń informatycznych", jest podstawą ewaluacji bezpieczeństwa produktów IT, zgodnie z metodyką opisaną w normie PN ISO/IEC 18045 „Metodyka oceny zabezpieczeń informatycznych". Na początku 2019 roku wspomniane normy międzynarodowe zostały też przyjęte jako normy europejskie (z prefiksem EN przed ISO/IEC). Z uwagi na powszechną percepcję, całość jest znana pod pojęciem norm serii ISO/IEC 15408 lub krótko, jako Common Criteria (CC).

Model bezpieczeństwa zastosowany w CC wynika z podstawowych zależności między czynnikami ryzyka w bezpieczeństwie informacji oraz metod szacowania, a następnie postępowania z ryzykiem (zob. Rysunek 1). W CC pojęcie samego bezpieczeństwa (security) nie zostało zdefiniowane, jednakże szereg definicji pojęć z nim związanych wskazuje na jego rozumienie jako zachowanie podstawowych atrybutów informacji takich jak poufność, integralność i dostępność. Dla celów CC definicje są węższe i prezentują funkcjonalny punkt widzenia w procesie definiowania, a następnie oceny bezpieczeństwa.

W celu zdefiniowania zbioru funkcjonalnych wymagań bezpieczeństwa, na poziomie abstrakcyjnym, w modelu bezpieczeństwa stosowanym w CC, operuje się pojęciem aktywów, które mają dla organizacji[2] określoną wartość. W wyniku działania czynników zagrożeń związanych z bezpieczeństwem informacji (zwanych w CC agentami zagrożeń) powstaje ryzyko, szacowane z uwzględnieniem prawdopodobieństwa zmaterializowania się zagrożenia oraz skutków/konsekwencji dla analizowanych aktywów, w wypadku tej materializacji. Szacowanie ryzyka powinno być podstawą do formułowania wymagań bezpieczeństwa dla konkretnych zastosowań modelu bezpieczeństwa, ponieważ to zabezpieczenia – rozumiane jako realizacja wymagań – mogą modyfikować ryzyka. Z uwagi na cechę charakterystyczną ryzyka, wyrażającego miarę niepewności osiągnięcia pożądanego stanu (rezultatu, celu), w modelu bezpieczeństwa stosowanym w CC uwzględnia się ocenę bezpieczeństwa, rozumianą jako pewność zastosowania wystarczających zabezpieczeń i zapewnienie poprawności funkcjonowania zabezpieczeń (zob. Rysunek 2).

Common Criteria to nie tylko metodyka oceny bezpieczeństwa, ale także metodyka tworzenia specyfikacji technicznej dla produktu w postaci funkcjonalnych wymagań bezpieczeństwa oraz wymagań uzasadnie-

[2] W CC używa się pojęcia właściciela aktywów; pojęcie organizacja jest ogólniejsze i preferowane w przyjętych w ostatnich latach modelach bezpieczeństwa, np. w ISO/IEC 27001.



Rysunek 2. Model oceny bezpieczeństwa zgodny z Common Criteria
Źródło: EN-ISO/IEC 15408-1

nia zaufania (ang. *assurance*) do samej oceny bezpieczeństwa, czyli zakresu, rygoru i wnikliwości oceny. Dodatkową cechą Common Criteria jest możliwość stworzenia dwóch typów specyfikacji technicznej:

– niezależnej od sposobu wdrożenia, w postaci **profilu zabezpieczeń** (PP – *Protection Profile*), czyli dla typu produktu
– zależnej od sposobu wdrożenia w postaci dedykowanej **specyfikacji zabezpieczeń** (ST – *Security Target*), czyli dla konkretnego produktu.

Specyfikacja ogólna PP (dla typu produktu, np. firewalla) może być podstawą dla dedykowanej specyfikacji ST (dla konkretnego produktu danego typu, np. firewall firmy X w wersji y.yy).

Oba typy specyfikacji technicznej mogą stać się podstawą dla produktu będącego **przedmiotem oceny** (TOE – Target of Evaluation). Dodatkowo, sama specyfikacja PP także może być takim przedmiotem oceny i zostać poddana ewaluacji na zgodność z Common Criteria. W następstwie pozytywnego rezultatu ewaluacji przedmiotu oceny uzyskuje się certyfikat.

2.5.2. Ewaluacja bezpieczeństwa produktu w Common Criteria

Jeśli klient jest zainteresowany niezależnym potwierdzeniem, że produkt, jakiego potrzebuje, spełnia wymagania bezpieczeństwa, to realizacja tej części procesu odbywa się zgodnie z systematyką opisaną w CC.

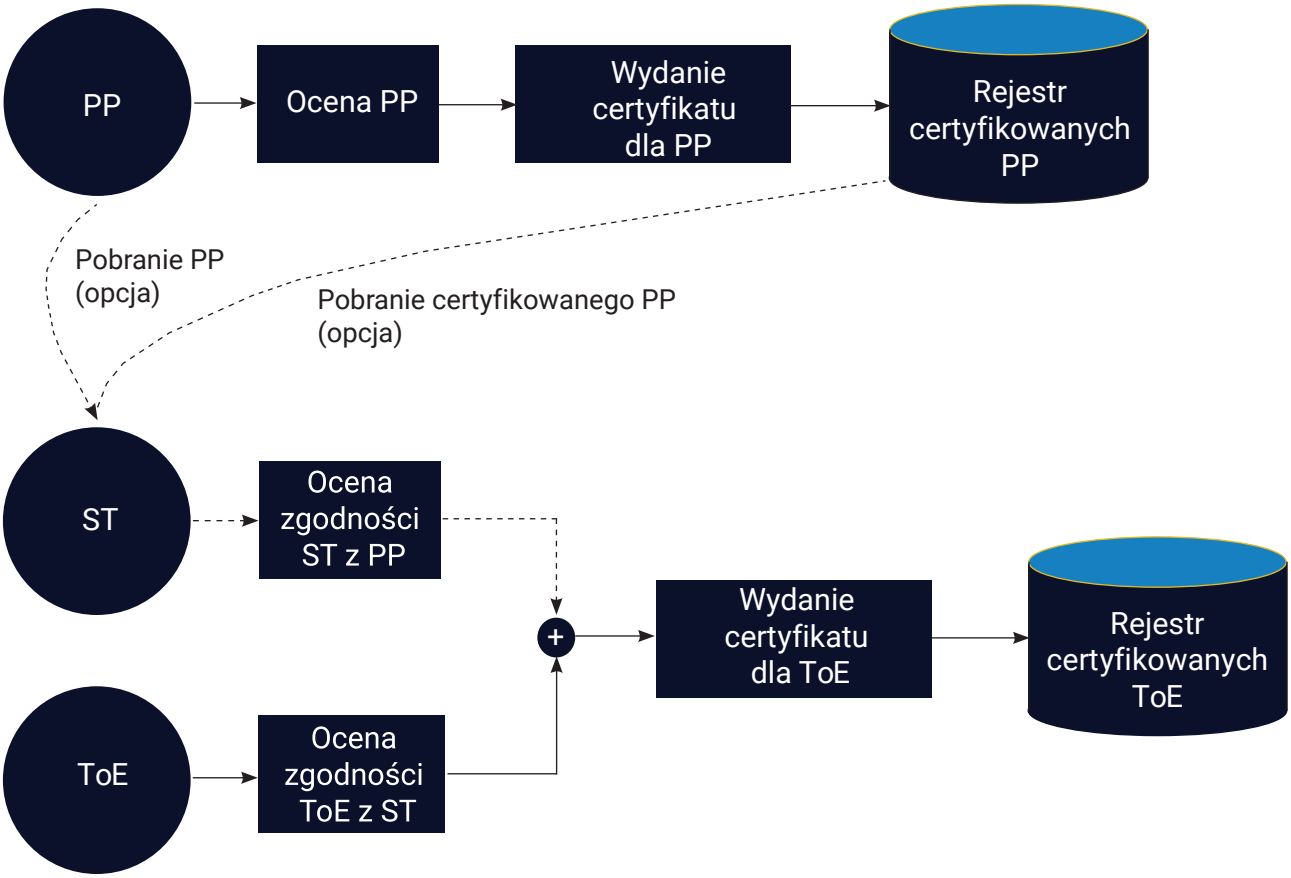
Przyjmując produkt do oceny opisany jako TOE, jednostka oceniająca stosuje metody przyjęte w CC (odpowiednie klasy dla PP i ST) do stwierdzenia, czy:

a) ST jest zgodny z PP,
b) TOE jest zgodny z ST.

W modelu, w którym produkt nie został zaprojektowany na podstawie PP, ocena ogranicza się do punktu b).

Należy wskazać, że ocena ta nie ma wartości absolutnej, tzn.:

– nie zapewnia, że wymagania klienta zostały poprawnie zapisane w PP lub ST,



Rysunek 3. Podstawowy schemat zależności PP od ST zgodnie z Common Criteria
Źródło: EN-ISO/IEC 15408-1

– stwierdzenia o zgodności mają poziom uzasadnionej pewności, uzależniony od zakresu, głębokości i rygoru oceny,
– ocena jest przeprowadzana przy uwzględnieniu szeregu warunków zawężających produkt IT do TOE.

Walor wartości oceny jest uzyskany dzięki przyjęciu CC jako normy międzynarodowej, międzypaństwowych porozumień o wzajemnym uznawaniu certyfikatów wydawanych na podstawie ocen bezpieczeństwa oraz powszechnej akceptacji rynku dla podejścia zgodnego z CC. Podstawowy schemat międzynarodowego uznania oceny bezpieczeństwa zgodnej z CC przedstawiono na Rys. 3 (linią przerywaną zaznaczono zależności, które nie muszą występować w każdej instancji procesu oceny i certyfikacji bezpieczeństwa produktu rozumianego jako przedmiot oceny).

Common Criteria ma siedem rosnących, poziomów uzasadnienia pewności zaufania (EALx, x =1,...7). Podmiot ubiegający się o certyfikat określa poziom EAL, który chce uzyskać i przedstawia dokumentację niezbędną do przeprowadzenia oceny bezpieczeństwa.

EAL1 – Przetestowany funkcjonalnie. Komponenty uzasadnienia zaufania: EAL1 zapewnia podstawowy poziom uzasadnienia zaufania, na podstawie analizy funkcjonalnych wymagań bezpieczeństwa (SFR) opisanych w ograniczonym ST, przeprowadzonej z użyciem specyfikacji funkcjonalnej interfejsów, wystarczających do zrozumienia charakterystyki bezpieczeństwa TOE.

EAL2 – przetestowany strukturalnie. Komponenty uzasadnienia zaufania: EAL2 zapewnia uzasadnienie zaufania przez pełny opis ST oraz analizę SFR, w tym ST na podstawie specyfikacji funkcjonalnej interfejsów, dokumentacji wytycznych oraz podstawowego opisu architektury, wystarczających do zrozumienia charakterystyki bezpieczeństwa TOE.

EAL3 – metodycznie sprawdzony i przetestowany. Komponenty uzasadnienia zaufania: EAL3 zapewnia uzasadnienie zaufania przez pełną analizę ST oraz analizę SFR, w tym ST na podstawie specyfikacji funkcjonalnej interfejsów, dokumentacji wytycznych oraz opisu architektury wykorzystanej do projektowania TOE, wystarczających do zrozumienia charakterystyki bezpieczeństwa TOE.

EAL4 – metodycznie projektowany, testowany i sprawdzony. Komponenty uzasadnienia zaufania: EAL4 zapewnia uzasadnienie zaufania przez pełną analizę ST oraz analizę SFR, w tym ST na podstawie specyfikacji funkcjonalnej interfejsów, dokumentacji wytycznych oraz opisu podstawowej, modułowej architektury wykorzystanej do projektowania TOE, wystarczających do zrozumienia charakterystyki bezpieczeństwa TOE.

EAL5 – półformalnie zaprojektowany i przetestowany. Komponenty uzasadnienia zaufania: EAL5 zapewnia uzasadnienie zaufania przez pełną analizę ST oraz analizę SFR, w tym ST na podstawie funkcjonalnej i kompletnej specyfikacji interfejsów, dokumentacji wytycznych, opisu podstawowej, modułowej architektury wykorzystanej do projektowania TOE oraz jego wdrożenia, wystarczających do zrozumienia charakterystyki bezpieczeństwa TOE. Wymagane jest modułowe projektowanie funkcji bezpieczeństwa TOE (TSF).

EAL6 – półformalnie zweryfikowany od strony projektowej i przetestowany. Komponenty uzasadnienia zaufania: EAL6 zapewnia uzasadnienie zaufania przez pełną analizę ST oraz analizę SFR w tym ST, na podstawie funkcjonalnej i kompletnej specyfikacji interfejsów dokumentacji wytycznych, projektu TOE i jego wdrożenia, wystarczających do zrozumienia charakterystyki bezpieczeństwa TOE. Ponadto wymagane jest modułowe i warstwowe projektowanie funkcji bezpieczeństwa TOE (TSF).

EAL7 – formalnie zweryfikowany od strony projektowej i przetestowany. Komponenty uzasadnienia zaufania: EAL7 zapewnia uzasadnienie zaufania przez pełną analizę ST oraz analizę SFR, w tym ST, na podstawie funkcjonalnej i kompletnej specyfikacji interfejsów, oraz strukturalnego wdrożenia, wystarczających do zrozumienia charakterystyki bezpieczeństwa TOE. Dodatkowe uzasadnienie zaufania jest osiągane przez formalny model wybranych polityk bezpieczeństwa TOE i półformalną prezentację specyfikacji funkcjonalnej i projektu TOE. Ponadto, wymagane jest modułowe i warstwowe projektowanie funkcji bezpieczeństwa TOE (TSF).

2.6. Schematy certyfikacji

Schematy certyfikacji[3] to struktury określające wymagania odnoszące się do procesu oceny zgodności. Obejmują one nie tylko odniesienie do norm referencyjnych, ale też określają właściciela schematu i model biznesowy schematu, wymagania organizacyjne i proceduralne związane z przeprowadzaniem oceny zgodności, struktury organizacji zarządzania certyfikatami i zasady działania tych struktur. W schemacie certyfikacji są zdefiniowane określone role w procesie.

W jednym schemacie ocenę zgodności (tzn. ewaluację i certyfikację) może w całości przeprowadzać jeden podmiot, zwany jednostką oceniającą zgodność wydającą certyfikaty, natomiast w innym role mogą być rozdzielone między niezależne podmioty, tzn. ewaluację przeprowadza wyspecjalizowane laboratorium, a certyfikat wydaje – na podstawie otrzymanego od laboratorium werdyktu – inny podmiot (jednostka certyfikująca). Przykładem pierwszego modelu jest schemat certyfikacji dla systemów zarządzania, natomiast drugiego – schemat certyfikacji zgodny z Common Criteria, w którym funkcjonują laboratoria ewaluacyjne (ITSEF – IT Security Evaluation Facility) oraz jednostka certyfikująca (CB – Certification Body).

CCRA (Common Criteria Recognition Arrangement)[4] skupia krajowe schematy oceny i certyfikacji zgodności z Commmon Criteria, które uznają wzajemnie wydawane przez siebie certyfikaty. Uczestnikami, którzy wydają certyfikaty są Australia, Kanada, Francja, Niemcy, Indie, Włochy, Japonia, Malezja, Holandia, Nowa Zelandia, Norwegia, Korea, Singapur, Hiszpania, Szwecja, Turcja i Stany Zjednoczone. CCRA uznaje certyfikaty do poziomu EAL2, przy czym każdy z badanych komponentów musi posiadać ALC_FLR, który stwierdza, że producent musi mieć opracowane procedury usuwania podatności w produkcie. Nie oznacza to, że wzajemne uznawanie certyfikatów dotyczy wyłącznie takich produktów, dla których przeprowadzono ocenę bezpieczeństwa na niskim poziomie uzasadnienia zaufania. W ramach CCRA uznawane są certyfikaty na dowolnie wysokim poziomie EAL, o ile produkty poddawane ewaluacji są zgodne z zatwierdzonym przez CCRA profilem zabezpieczeń. Te specyfikacje techniczne są opracowywane przez grupy eksperckie, funkcjonujące w ramach CCRA, w następujących obszarach bezpieczeństwa:

– Application Software
– Biometrics Security
– Database Management Systems
– Dedicated Security Components
– Full Disk Encryption
– Network Fundamentals and Firewall
– USB Portable Storage Devices

Efektem prac grup technicznych są specyfikacje techniczne, które noszą nazwę cPP (*collaborative Protec-*

[3] W literaturze przedmiotu jest używane także pojęcie „program certyfikacji", w tym kontekście równoważne ze „schematem certyfikacji".

[4] Za Common Criteria Portal, https://www.commoncriteriaportal.org/ oraz https://www.sogis.eu/, dostęp 10.12.2019 r.

tion Profile). Należy wskazać, że na dziś liczba certyfikowanych cPP jest ograniczona do:

– dwóch specyfikacji dot. firewalla realizującego funkcje statycznego filtrowania ruchu
– czterech specyfikacji dotyczącej całkowitego szyfrowania dysków
– trzech specyfikacji dla urządzeń sieciowych

Niemniej, w każdej z wyżej wymienionych grup eksperckich trwają prace nad następnymi cPP, a efekty tych prac są publicznie dostępne, co spowoduje w przyszłości zwiększenie liczby wzajemnie uznawanych certyfikatów, wydawanych pod marką CCRA.

W Europie podobną rolę odgrywa porozumienie o wzajemnym uznawaniu certyfikatów **SOG-IS MRA** (Senior Officials Group – Information Security Systems Mutual Recognition Agreement), skupiający 17 krajów europejskich. Członkowie SOG-IS uznają wzajemnie certyfikaty do poziomu EAL4.
Zarówno w CCRA, jak i w SOG-IS, uczestnik może mieć jeden z następujących statusów:

– Consumer Participant, czyli uczestnik jedynie uznający certyfikaty wydawane przez innych,
– Authorized Participant, czyli uczestnik wydający i uznający certyfikaty.

Dodatkowo w ramach SOG-IS istnieje podgrupa uczestników o statusie:

– Qualified Participant, który to status jest możliwy do uzyskania jedynie przez Authorized Participant i pozwala na wydawanie certyfikatów w dwóch domenach technicznych: kart elektronicznych oraz urządzeń z wbudowanym modułem kryptograficznym do poziomu EAL7.

Zmiana statusu na uczestnika wydającego certyfikaty jest możliwa po spełnieniu szeregu wymagań odnośnie zdolności technicznych, proceduralnych i organizacyjnych opisanych w porozumieniach. Polski schemat oceny i certyfikacji cyberbezpieczeństwa KSO3C jest konsumentem certyfikatów w SOG-IS od kwietnia 2017 roku, a w CCRA od grudnia 2018 roku.
Warto podkreślić, że w ramach CCRA i SOG-IS MRA certyfikaty są wzajemnie uznawane – jeśli dotyczą produktów zgodnych z określonym i certyfikowanym profilem zabezpieczeń – do poziomu EAL4. Takie certyfikaty są oznaczone znakiem obu porozumień. W wypadku, gdy dla przedmiotu oceny nie ma deklaracji zgodności z profilem zabezpieczeń, to wzajemne uznawanie certyfikatów w CCRA jest ograniczone do poziomu EAL2. SOG-IS nie wprowadził takich ograniczeń w swoim systemie wzajemnego uznawania certyfikatów jak CCRA.

Diagnoza stanu obecnego – przegląd stosowanych standardów w obszarze bezpieczeństwa Teleinformatycznego w sektorze bankowym

3.1. Wprowadzenie

Źródła wymagań bezpieczeństwa w sektorze bankowym mogą być różnorakie: akty prawne, regulacje sektorowe, jednakże oceny bezpieczeństwa w kontekście certyfikacji mogą być przeprowadzane jedynie wobec jednoznacznie określonej specyfikacji technicznej, opisanej np. w normach międzynarodowych lub standardach branżowych. Nie umniejsza to w żadnym względzie znaczenia warstwy legislacyjnej lub regulacyjnej, z której wynika konieczność zastosowania określonej specyfikacji technicznej w celu przeprowadzenia oceny zgodności.

W tym rozdziale zostanie omówiona warstwa legislacyjna oraz regulacyjna odnosząca się wprost do cyberbezpieczeństwa oraz normy międzynarodowe i standardy branżowe będące podstawą certyfikacji w obszarze cyberbezpieczeństwa.

3.2. Akty prawne regulujące podejście do cyberbezpieczeństwa w sektorze bankowym

Kwestia bezpieczeństwa danych przetwarzanych przez podmioty sektora bankowego, w tym: cyberbezpieczeństwa w systemach informatycznych z dostępem do Internetu, znajduje się wysoko na liście priorytetów Unii Europejskiej. Wprowadzona w ostatnich latach unijna legislacja, a w ślad za nią krajowe akty prawne wdrażające legislacje unijne, określają wysokopoziomowe wymagania bezpieczeństwa i silnie regulują zachowanie podmiotów w sektorze finansowym.

Dyrektywa NIS[5] odnosi się do cyberbezpieczeństwa sieci i systemów informatycznych. Wdrożeniem Dyrektywy NIS do prawa krajowego jest ustawa o Krajowym Systemie Cyberbezpieczeństwa[6]. Ustawa wprowadza szereg wymagań dla operatorów usług kluczowych, w zakresie opracowania i wdrażania strategii cyberbezpieczeństwa, zarządzaniem ryzykiem w obszarze cyberbezpieczeństwa czy raportowania zdarzeń uznanych za incydenty związane z cyberbezpieczeństwem. Ponieważ banki podlegają podmiotowo przepisom ustawy jako operatorzy usług kluczowych, to mają obowiązek spełnienia powyższych wymagań. Operatorów usług kluczowych w sektorze bankowym wyznacza Komisja Nadzoru Finansowego.

Dyrektywa PSDII[7] (Dyrektywa o Usługach Płatniczych) dotyczy stricte sektora bankowego i skupia się na ochronie konsumenta przy transakcjach bezgotówkowych, wprowadzając wymagania cyberbezpieczeństwa w obszarze komunikacji elektronicznej i aplikacjach płatności w Internecie oraz dostępu nowych podmiotów do tych usług (system otwartej bankowości). Wdrożenie Dyrektywy do prawa krajowego nastąpiło przez zmiany w ustawie o usługach płatniczych. Wymagania dotyczące mechanizmów silnego uwierzytelniania stron transakcji bezgotówkowej i bezpiecznej komunikacji między stronami, mające zastosowania w sektorze bankowym, sformułowała również organizacja skupiająca krajowe organy nadzoru finansowego (Europejski Urząd Nadzoru Bankowego/EBA), w postaci Regulatory Technical Standards, towarzyszących PSDII. Kwestia dostępu do systemów bankowych przez strony trzecie powoduje wzrost ryzyka naruszenia cyberbezpieczeństwa. Certyfikacja platform świadczenia usług płatniczych lub interfejsów łączących systemy bankowe z systemami zewnętrznych usługodawców może ograniczać ryzyka związane z cyberbezpieczeństwem, co spowoduje wzrost zaufania do nowych systemów płatniczych zarówno regulatora, jak i konsumenta.

Rekomendacje KNF[8]. Komisja Nadzoru Finansowego sprawuje nadzór nad systemem finansowym w Polsce. Wydaje ona Rekomendacje w różnych sferach funkcjonowania tegoż systemu. Dla podmiotów objętych nadzorem stosowanie się do Rekomendacji jest obowiązkowe i regularnie kontrolowane. Najistotniejsze w kontekście cyberbezpieczeństwa są: Rekomendacja D (dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach) oraz Rekomendacja M (zarządzanie ryzykiem operacyjnym). KNF regularnie uaktualnia Rekomendacje, i biorąc pod uwagę priorytety polityki UE w postaci rozwoju innowacyjnych technologii cyfrowych oraz zwiększania zaufania do bezpieczeństwa nowych technologii, można spodziewać się powstawania programów certyfikacyjnych dla tych rozwiązań.

Rekomendacje KNF nie są standardami w rozumieniu norm międzynarodowych, nie wydaje się na ich podstawie certyfikatów, jednak pełnią podobną funkcję w tym sensie, że regulator okresowo przeprowadza kontrolę stosowania się podmiotu do zapisów rekomendacji.

[5] https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX%3A32016L1148 dostęp 1.11.2019 r.
[6] http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001560/T/D20181560L.pdf dostęp 1.11.2019 r.
[7] https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32015L2366&qid=1576595443499&from=EN dostęp 1.11.2019 r.
[8] https://www.knf.gov.pl/dla_rynku/regulacje_i_praktyka/rekomendacje_i_wytyczne/rekomendacje_dla_bankow?articleId=8522&p_id=18 dostęp 2.11.2019 r.

3.3. Standardy branżowe w certyfikacji produktów na użytek sektora bankowego

3.3.1. Certyfikaty EMVCo[9]

EMVCo to międzynarodowa organizacja założona przez sześciu głównych operatorów płatności (American Express, Discover, JCB, Mastercard, UnionPay i Visa), której zadaniem jest tworzenie i rozwijanie standardów bezpiecznych transakcji (nazywanych Specyfikacjami EMV).

EMVCo wydało i aktualizuje szereg **Specyfikacji**, dotyczących konkretnych typów produktów, wykorzystywanych w płatnościach. Organizacja definiuje swoje specyfikacje jako „technologiczny zestaw narzędzi, który umożliwia globalnie interoperacyjne, bezpieczne płatności w bezpośrednich i zdalnych środowiskach". Specyfikacje muszą być spełnione przez produkty wykorzystywane przy transakcjach z udziałem sygnatariuszy EMVCo. Produkt musi przejść ewaluację bezpieczeństwa przeprowadzaną zgodnie z procedurami organizacji, przez jedno z 12 laboratoriów zaakceptowanych przez EMVCo. Ewaluacji bezpieczeństwa może być poddany jeden z trzech typów produktów:

1. **Integrated Circuit (IC)** – układ mikroprocesorowy wraz z oprogramowaniem (firmware) lub bibliotekami, które umożliwiają dostęp do funkcji bezpieczeństwa układu mikroprocesorowego oraz towarzyszącą dokumentacją.

2. **Platforma**, która jest budowana na układzie mikroprocesorowym i składa się z następujących komponentów:

   - obszaru pamięci przeznaczonego do bezpiecznego składowania i wykonywania poleceń z aplikacji, zarządzanie przez system operacyjny Platformy
   - usługi Platformy dla aplikacji
   - usługi zarządzania zawartością karty, w tym:
     - zarządzania bezpieczeństwem (np. ładowanie aplikacji, zamykanie karty)
     - domeny bezpieczeństwa dla Platformy w wypadku wielu dostawców (aplikacji)
     - bezpiecznej komunikacji między obiektami osadzonymi na karcie oraz systemami zewnętrznymi w stosunku do karty
     - towarzyszącej dokumentacji Platformy.

Ewaluacja bezpieczeństwa może dotyczyć dwóch konfiguracji Platformy:
- otwartej – ładowanie aplikacji i instalacja w docelowej lokalizacji jest możliwa podczas fazy użytkowania Platformy
- zamkniętej – ładowanie aplikacji i instalacja jest nieaktywna podczas fazy personalizacji, tak więc żadna aplikacja nie może zostać zainstalowana poza lokalizacją wytwórcy Platformy; Platforma jest traktowana jako produkt końcowy.

3. Karta mikroprocesorowa – składająca się z układu mikroprocesorowego, systemu operacyjnego i dodatkowych usług np. zarządzania aplikacjami (Platformy) oraz aplikacji płatniczej.

Struktura organizacyjna EMVCo, określana jako Sekretariat Ewaluacji, ocenia raport z ewaluacji bezpieczeństwa pod kątem merytorycznym i wydaje certyfikat zgodności ze specyfikacjami. Metodyka i terminologia procesu ewaluacji układu mikroprocesorowego oraz Platformy dla kart inteligentnych jest identyczna, jak w Common Criteria na poziomach uzasadnienia zgodności EAL4+ i EMVCo uznaje certyfikaty CC za równoważne. Certyfikat pozwala na wprowadzenie na rynek produktu z marką jednego z udziałowców EMVCo.

Z uwagi na dominującą pozycję uczestników EMVCo na rynku globalnym operatorów systemów płatniczych, organizacja ta określa zarówno specyfikacje wymagań bezpieczeństwa dla produktów przeznaczonych dla sektora bankowego, jak i system weryfikacji spełniania tych wymagań za pośrednictwem sieci akredytowanych przez siebie laboratoriów oceny bezpieczeństwa oraz wydaje certyfikaty. W efekcie banki są zmuszone do stosowania takich produktów, nie mając wpływu na system weryfikacji ich bezpieczeństwa.

3.3.2. Specyfikacje EMVCo

Specyfikacje w ramach EMVCo to zbiór ściśle technicznych wymagań dla produktów. Poniżej zostały omówione okoliczności ich wykorzystywania oraz przydatność certyfikatów dla konsumentów.

Contact EMV to pierwsza w historii EMVCo, najstarsza specyfikacja dla produktów płatniczych, wykorzystujących układ mikroprocesorowy (chip). Obecnie obowiązująca specyfikacja to już wersja 4.3. Contact EMV określa, jak bezpiecznie przeprowadzać transakcje z wykorzystaniem karty z chipem, którą należy umieścić w terminalu płatniczym. Certyfikowane karty posiadają funkcje kryptograficzne, w celu zapobieżenia podrabianiu kart i szereg zabezpieczeń gwarantujących wyższe bezpieczeństwo niż w przypadku kart z paskiem magnetycznym.

Contactless EMV to specyfikacja dotycząca produktów wykorzystywanych przy transakcjach bezstykowych, opartych na technologii zbliżeniowej NFC.

[9] Dwa podrozdziały na podstawie treści oraz dokumentów portalu https://www.emvco.com/ dostęp 30.10.2019 r.

Karta bezstykowa umożliwia realizację transakcji płatniczej, dzięki przybliżeniu karty do terminala obsługującego EMV Contactless. Szczegółowe specyfikacje gwarantujące bezpieczeństwo są podobne do Contact EMV, zatem podobnie certyfikowane produkty są bezpieczniejsze niż karty z paskiem magnetycznym. Obecnie specyfikacja jest w wersji 2.8.

Mobile EMV to specyfikacja związana z płatnościami realizowanymi za pomocą aplikacji mobilnej zainstalowanej na smartfonie, jednej z najszybciej rozwijających się metod płatności. Zastosowanie aplikacji mobilnej w płatnościach może być różnorakie, od zastąpienia bądź uzupełnienia fizycznych kart zbliżeniowych, po realizację funkcji terminala płatniczego dla sprzedawcy. Poza zastąpieniem kart zbliżeniowych, telefony mogą być wykorzystywane również do optycznego przechwytywania płatności, wykorzystywanego zarówno w płatnościach mobilnych, jak i w transakcjach przy wykorzystaniu urządzeń mobilnych. Na podstawie tej specyfikacji można tworzyć funkcjonalności z wykorzystaniem urządzeń Internetu Rzeczy i potencjalnych płatności z użyciem urządzeń tego typu.

EMV Payment Tokenisation to specyfikacja opisująca dodatkową funkcjonalność tokenizacji, zwiększającą bezpieczeństwo transakcji internetowych. Tokenizacja polega na zamianie wrażliwych danych na token, czyli ciąg cyfr, i używania takiego tokenu podczas przesyłania danych. Tokeny mogą być przypisane do konkretnego urządzenia, np. telefonu, konkretnego sprzedawcy detalicznego, np. gdy numer karty zapisany jest w sklepie internetowym, albo konkretnego sposobu użytkowania, np. płatności w Internecie kartą. W przypadku utraty urządzenia bądź wykradzenia danych ze sklepu internetowego, możliwe jest zastrzeżenie samego tokenu, a nie całej karty. Podobnie przy zastrzeżeniu zgubionej karty, konsument może wciąż korzystać z tokenów. System tokenizacji płatności nie jest odrębny od pozostałych systemów płatności, raczej stanowi nakładkę wspierającą handel internetowy i nowe metody płatności. Korzystanie z tokenów zwiększa bezpieczeństwo systemu płatniczego, choć jednocześnie wprowadza nowe wyzwania w postaci np. braku pełnej historii transakcji. Długoterminowe rozwiązanie tego problemu polega na odejściu od rejestracji płatności konkretną kartą i przejście do rejestracji przez numer rachunku płatniczego.

EMV QR Code to specyfikacja użycia QRCode w transakcjach płatniczych, zarówno po stronie konsumenta, jak i sprzedawcy. QR Code jest metodą wizualizacji danych wykorzystywaną w wielu sektorach, opisaną w normie ISO 18004. Odpowiednio skonstruowany kod QR, po zeskanowaniu telefonem kontrahenta, pozwala na wykonanie płatności bez wykorzystywania urządzeń ani łączenia się między nimi. EMVCo nie zapewnia oceny zgodności urządzeń wykorzystujących kody QR, choć istnieje możliwość ewaluacji konkretnego kodu QR bądź otrzymania przykładowych kodów.

EMV® Secure Remote Commerce (SRC) to zbiór specyfikacji pozwalający na stworzenie „wirtualnego terminala płatniczego". Pod tą nazwą zebrane są wszystkie transakcje, w których klient nie ma bezpośredniej, fizycznej interakcji z terminalem, czyli np. zakupy przez Internet. Punktem krytycznym procesu jest moment, w którym kupujący musi podać dane swojego środka płatniczego w celu przeprowadzenia transakcji. EMV SRC stanowi podstawę dla rozwijanych przez biznes platform przetwarzania transakcji, bez względu na urządzenie wykorzystane do ich zlecenia, czy to telefon, komputer czy tablet. EMV SRC tworzy jednolite, uproszczone środowisko realizacji płatności, zabezpiecza obie strony transakcji i obsługuje różne typy urządzeń (w tym IoT). Specyfikacje określają interfejsy klienta, aplikacji i komunikacji między nimi oraz wprowadzają kompatybilność z innymi technologiami, takimi jak tokenizacja czy 3-D Secure.

EMV® 2nd Generation (2nd Gen) – specyfikacje tej grupy są uaktualnieniem specyfikacji akceptacji płatności (w tym EMV Contact i EMV Contactless), tak aby były one kompatybilne z nowoczesnymi, elastycznymi i modułowymi platformami płatniczymi. Stanowią one rozszerzenie istniejących specyfikacji, jednak ich nie zastępują. Modułowa konstrukcja terminali pozwala na obsługiwanie różnych środowisk, przepływów i protokołów. Druga generacja specyfikacji umożliwia zintegrowane testowanie różnych kanałów płatności przez posiadanie jednego jądra dla różnych interfejsów.

EMV 3-D Secure specyfikacja EMV 3-D Secure zapewnia uwierzytelnianie transakcji w aplikacji mobilnej i integrację z portfelem mobilnym. Protokół 3DS powstał w firmie VISA w celu zwiększenia bezpieczeństwa transakcji internetowych przez dodanie warstwy uwierzytelniania. EMV Three-Domain Secure (3DS) to protokół przesyłania wiadomości opracowany przez EMVCo, pozwalający klientom uwierzytelnić się u wydawcy karty podczas dokonywania transakcji internetowych z wykorzystaniem PAN lub tokenu płatniczego. Trzy domeny to: domena sprzedawcy/ nabywcy, domeny emitenta środka płatniczego i domeny interoperacyjności, np. systemu płatności.

Jak wskazano w rozdziale 3.3.1, system weryfikacji zgodności ze specyfikacjami wymagań bezpieczeństwa EMVCo jest zarządzany przez EMVCo, bez niezależnej kontroli zewnętrznej (np. regulatorów czy klientów, czyli podmiotów sektora bankowego).

Z uwagi na konieczność zapewnienia wymiany informacji między systemami bankowymi, rozwiązania teleinformatyczne stosowane w bankach wykorzystują produkty zatwierdzane przez EMVCo.

3.3.3. Standardy PCI SSC[10]

Organizacja **Payment Card Industry Security Standards Council** (PCI SSC) powstała w 2006 roku jako wspólna inicjatywa American Express, Discover, JCB International, MasterCard i Visa.

Powstające w jej ramach standardy branżowe odnoszą się do bezpieczeństwa danych gromadzonych w trakcie procesu płatności, w tym danych posiadacza karty płatniczej. Głównym standardem jest PCI Data Security Standard. Dodatkowo powstało kilkanaście uzupełniających specyfikacji, dotyczących bezpieczeństwa elementów płatności lub rozwijających zapisy PCI DSS, jak np. Pin Security, Payment Application Data Security Standard. Uzupełniające specyfikacje są ściśle techniczne. Organizacja PCI SSC certyfikuje zarówno podmioty, jak również ich rozwiązania na zgodność ze swoimi specyfikacjami technicznymi. Ocenę zgodności realizują laboratoria uznane (akredytowane) przez PCI, które są wtedy określane jako Qualified Security Assessor (QSA).

PCI Data Security Standard (PCI DSS). PCI DSS to standard dedykowany do organizacji. Został stworzony, by poprawić bezpieczeństwo danych klienta – posiadacza karty. Składa się z 14 podstawowych wymagań, które można ująć w sześciu kategoriach:

– budowa i utrzymanie bezpiecznej sieci
– ochrona danych posiadacza karty
– wdrożenie programu zarządzania podatnościami
– wprowadzenie bezpiecznego zarządzania dostępem
– regularne sprawdzanie i testowanie bezpieczeństwa sieci
– wdrożenie polityki zarządzania bezpieczeństwem informacji.

Uzyskanie certyfikatu poświadczającego zgodność z PCI DSS jest obowiązkowe dla organizacji, które przechowują, przetwarzają lub przekazują dane związane z płatnościami lub dane mogące wpłynąć na bezpieczeństwo danych posiadaczy kart. Wśród nich są banki, organizacje wydające karty, operatorzy płatności czy sieci handlowe. W zależności od liczby transakcji miesięcznie, wymagany jest inny poziom certyfikacji.

Zgodność z PCI DSS określana jest przez organizację płatniczą, będącą członkiem Rady, nie przez samą radę. Wszyscy członkowie Rady PCI stosują tę samą metodykę oceny zgodności.

W odniesieniu do produktów PCI SSC opracowała szereg specyfikacji technicznych, z których najważniejsze omówiono poniżej.

Payment Application Data Security Standard (PA -DSS) to standard zawierający wymagania bezpieczeństwa dla aplikacji obsługujących płatności. Aktualna wersja PA-DSS (v3.2) określa 14 wymagań odnoszących się do sposobu działania aplikacji obsługującej płatność, których wdrożenie jest weryfikowane podczas oceny zgodności:

1. Nie przechowuj pełnych danych ze ścieżki, kodów weryfikacji karty lub wartości (CAV2, CID, CVC2, CVV2) lub danych blokowych PIN
2. Chroń dane posiadacza karty, które są przechowywane
3. Zapewnij sposoby bezpiecznego uwierzytelnienia
4. Zapisuj dane o aktywnościach aplikacji obsługującej płatności
5. Opracuj bezpieczne aplikacje obsługujące płatności
6. Chroń bezprzewodową transmisję
7. Testuj aplikacje obsługujące płatności w celu określenia podatności i utrzymuj system aktualizacji aplikacji obsługujących płatności
8. Używaj bezpiecznych konfiguracji sieci
9. Dane posiadaczy kart nie mogą być przechowywane na serwerze dołączonym do Internetu
10. Używaj zabezpieczonego zdalnego dostępu do aplikacji obsługującej płatności
11. Szyfruj transmisję danych wrażliwych realizowaną przez sieci publiczne
12. Zabezpiecz dostęp administracyjny, który jest realizowany poza konsolą administracyjną
13. Zapewnij wytyczne do wdrożenia PA-DSS klientom, partnerom handlowym i integratorom
14. Przypisz personelowi odpowiedzialności związane z PA-DSS oraz zapewnij program szkoleń dla personelu, klientów, partnerów handlowych i integratorów.

Obecnie jest 679 certyfikowanych aplikacji (stan na 6 grudnia 2019).

PCI PTS Hardware Security Modeles (HSM) Security Requirements to wymagania dla modułów kryptograficznych wykorzystywanych w procesach płatności. Ocena bezpieczeństwa wykonywana jest przez niezależne laboratoria i obejmuje wymagania bezpieczeństwa w odniesieniu do parametrów fizycznych, logicznych oraz zabezpieczeń samego urządzenia. Zgodność z wymaganiami dot. HSM jest wymagana do potwierdzenia zgodności z PCI DSS.

[10] Podrozdział na podstawie treści i dokumentów portalu https://www.pcisecuritystandards.org/ dostęp 30.10.2019 r.

PCI PIN Transaction Security Point of Interaction Security (PCI PTS POI) to standard dla produktów, które uczestniczą w zarządzaniu numerem PIN, podawanym przez klienta podczas transakcji kartą płatniczą, zarówno on-line jak i off-line. Terminale płatnicze i bankomaty podlegają ewaluacji na zgodność z PCI PTS POI.

Należy odnotować dominację organizacji ponadnarodowej, jaką jest PCI SSC w obszarze usług płatniczych i aplikacji płatniczych. PCI określa specyfikacje techniczne, udziela akredytacji podmiotom sprawdzającym zgodność z tymi specyfikacjami, a następnie akceptuje świadczenie usług płatniczych jedynie przez tych operatorów, w tym banki, którzy otrzymali certyfikat od PCI. Analogicznie, jak w wypadku EMVCo system ten ma charakter zamknięty, bez niezależnej kontroli ze strony regulatorów lub banków.

3.3.4. Harmonizacja wymagań bezpieczeństwa w SEPA

W różnych krajach europejskich (Francja, Niemcy, Wielka Brytania), równolegle do EMVCo, były rozwijane krajowe schematy oceny bezpieczeństwa rozwiązań w obszarze płatności elektronicznych.

W celu ułatwienia realizacji płatności elektronicznych, krajowych i transgranicznych w 2010 roku European Payment Council otworzył inicjatywę SEPA Card Framework (SCF), w której opracowano rozwiązania bazujące na normach międzynarodowych w odniesieniu do kart płatniczych oraz krytycznych komponentów terminali płatniczych lub bankomatów (ATM). W ramach SCF działa grupa Common Approval Scheme (CAS).

Celem prac CAS było zharmonizowanie wymagań bezpieczeństwa w europejskim systemie płatniczym działającym w obrębie SEPA. W tym celu grupa opracowała profil zabezpieczeń dla terminali płatniczych (Point of Interaction – POI PP) oraz kilka PP towarzyszących.

W profilu POI PP zidentyfikowano 6 podstawowych konfiguracji. Każda z tych konfiguracji jest opisana jako odrębny przedmiot oceny w postaci terminala płatniczego, wyposażonego w układ mikroprocesorowy, umożliwiającego przetwarzanie transakcji płatniczych zarówno w trybie on-line, jak i off-line. Zakres produktów poddanych ocenie bezpieczeństwa zgodnie z POI PP obejmuje proste terminale PED (PIN Entry Device), z klawiaturą, wyświetlaczem oraz czytnikami karty inteligentnej i karty z paskiem magnetycznym, oraz złożone urządzenia, które umożliwiają przetwarzanie danych związanych z transakcjami oraz mają możliwość komunikacji z innymi systemami.

Podstawowe konfiguracje POI obejmują:

1. **PED-ONLY** – taki przedmiot oceny ma zastosowanie, gdy PED jest komponentem innego bardziej złożonego urządzenia wykorzystywanego w transakcjach płatniczych, które samo może wymagać certyfikacji, jednakże z uwagi na powtarzalność tego komponentu warto poddać go oddzielnej ewaluacji, a jej wyniki użyć przy ewaluacji złożonej.

2. **POI-COMPREHENSIVE** – przedmiot oceny, w którym PED-ONLY jest rozszerzony o funkcje zarządzania danymi dotyczącymi transakcji płatniczych oraz funkcje komunikacji z zewnętrznymi urządzeniami służącymi do wymiany danych z Akceptantem.

3. POI-CHIP-ONLY – przedmiot oceny jest podzbiorem POI-Comprehensive, ponieważ nie zawiera wymagań bezpieczeństwa sprzętowego dla ochrony PIN oraz – w przeciwieństwie do pozostałych dwóch typów – nie obsługuje czytnika kart z paskiem magnetycznym. Należy zwrócić uwagę, że ten typ terminala nie przechowuje PIN w postaci niezaszyfrowanej.

W wypadku, gdy PP POI jest rozszerzony o opracowany przez PCI profil zabezpieczeń Open Protocol Package, czyli zbiór funkcji zapewniający bezpieczną komunikację urządzeń przetwarzających PIN ze światem zewnętrznym za pośrednictwem sieci publicznych, z trzech wyżej opisanych konfiguracji otrzymujemy 6 podstawowych konfiguracji przedmiotu oceny w obszarze terminali płatniczych.

Ocena zgodności i certyfikacja terminali płatniczych jest realizowana w ramach SOG-IS (zob. rozdział 2.6). W 2016 roku CAS zmieniła się w CSG (Cards Standardization Group), a następnie w ECSG (European Card Standardization Group). Jednym z obszarów działania ECSG jest standaryzacja rozwiązań bezpieczeństwa. ECSG blisko współpracuje z PCI, adaptując standardy wypracowane przez branżę (zob. Rozdział 3.3.3) do potrzeb europejskiego sektora elektronicznych transakcji płatniczych.

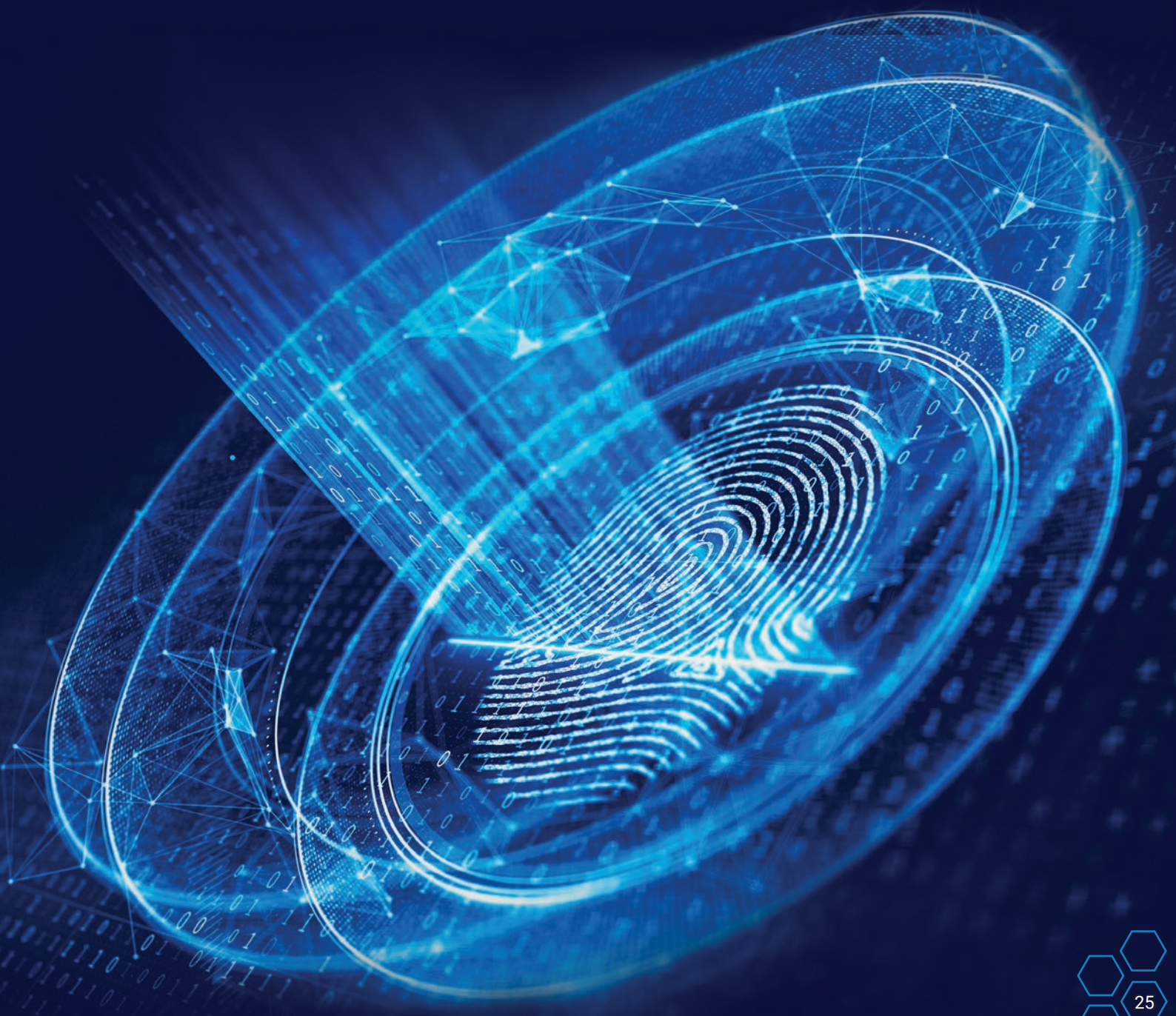
W przeciwieństwie do organizacji ponadnarodowych, takich jak EMVCo i PCI SSC, istniejący w Europie system bezpieczeństwa rozwiązań w obszarze usług płatniczych charakteryzuje się rozdzieleniem funkcji opracowywania specyfikacji bezpieczeństwa od ich weryfikowania, co pozytywnie wpływa na zaufanie rynku do rozwiązań oferowanych przez banki, jednakże prace w ramach SEPA nie mają udziału w rynku porównywalnego z EMVCo i PCI SSC.

3.3.5. Przyszłość certyfikacji w sektorze bankowym

Opisane powyżej systemy certyfikacji są obowiązkowe dla podmiotu, który chce wydać instrument płatniczy lub świadczyć usługi płatnicze we współpracy z EMVCo czy PCI. W wypadku EMVCo, 99% transakcji płatniczych w Europie odbywa się za pomocą instrumentów zgodnych ze specyfikacjami określonymi przez EMVCo i certyfikowanych przez EMVCo.

W kontekście zmian, jakie wynikają z Aktu o Cyberbezpieczeństwie (patrz Rozdział 4.), warto jednak zauważyć, że są to certyfikaty wydawane przez podmioty prywatne, a jako takie nie będą uznawane w ramach ogólnoeuropejskichnijnych schematów certyfikacji. Ze względu na silną pozycję podmiotów tworzących wyżej wymienione organizacje można spodziewać się specjalnych rozwiązań w zakresie certyfikacji instrumentów płatniczych, wynikających z kompromisów, jakie zostaną wypracowane przez strony (tzn. Komisję Europejską i wymienione organizacje ponadnarodowe), i pod warunkiem ich zaakceptowania przez sektor bankowy i konsumentów.

Znaczenie unijnego Rozporządzenia 2019/881 (CSA) dla podniesienia poziomu cyberbezpieczeństwa na Jednolitym Rynku Cyfrowym



4.1. Wprowadzenie

Rozporządzenie 2019/881 (CSA – Akt o Cyberbezpieczeństwie) weszło w życie 27 czerwca 2019 roku i jest drugą, po dyrektywie NIS, ogólnoeuropejską, horyzontalną regulacją kwestii cyberbezpieczeństwa. CSA składa się z dwóch części: pierwsza jest poświęcona ENISA (Agencji UE ds. Cyberbezpieczeństwa), druga ustanawia europejskie ramy certyfikacji cyberbezpieczeństwa.

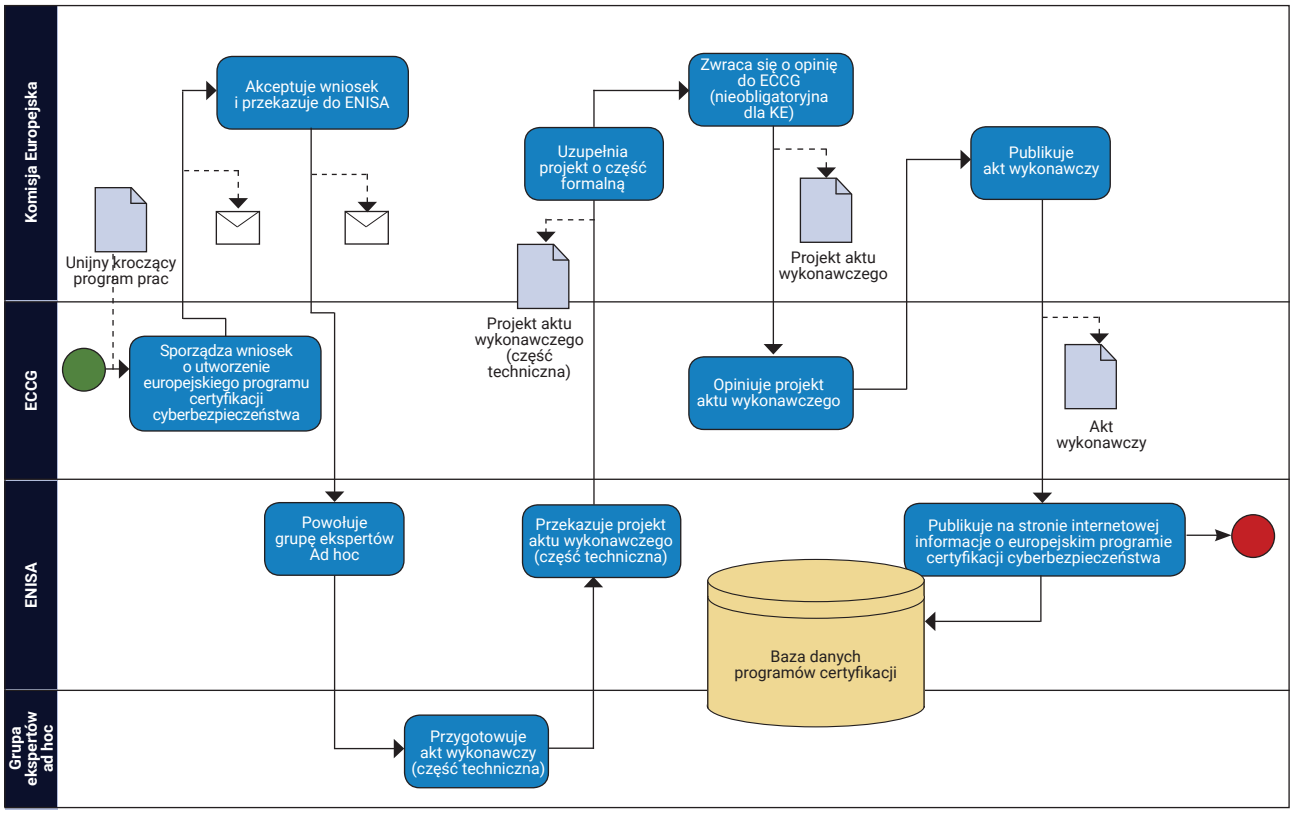
Celem CSA jest unifikacja certyfikacji cyberbezpieczeństwa w UE, pozwalająca na swobodniejszą współpracę i handel ponadnarodowy, oparty na zaufaniu do wzajemnie uznawanego certyfikatu cyberbezpieczeństwa.

W CSA zakłada się, że certyfikacji cyberbezpieczeństwa będą poddawane:

- produkty ICT, rozumiane jako elementy lub grupy elementów sieci lub systemów informatycznych;
- usługi ICT, rozumiane jako usługi polegające w pełni lub głównie na przekazywaniu, przechowywaniu, pobieraniu lub przetwarzaniu informacji za pośrednictwem sieci i systemów informatycznych;
- procesy ICT, rozumiane jako zestaw czynności wykonywanych w celu projektowania, rozwijania, dostarczania lub utrzymywania produktów ICT lub usług ICT;

Programy certyfikacji, funkcjonujące na podstawie CSA, zapewniające wzajemnie uznawane w Europejskim Obszarze Gospodarczym certyfikaty cyberbezpieczeństwa są wskazane jako jeden z fundamentów Jednolitego Rynku Cyfrowego, szerszej inicjatywy UE dążącej do cyfryzacji gospodarki.

Komisja Europejska publikuje, nie rzadziej niż co 3 lata, unijny kroczący program prac, wskazujący priorytetowe obszary dla ustanawiania programów certyfikacji. Priorytety określa się na podstawie kilku czynników: ryzyka rozdrobnienia certyfikacji w danym obszarze (np. poprzez powstawanie krajowych programów certyfikacji), znaczenia dla polityki Unii, popytu na certyfikację lub szczególnej podatności na cyberzagrożenia. Pierwszy program kroczący zostanie opublikowany w czerwcu 2020 roku. Na wniosek Komisji, ENISA przygotowuje propozycję programu certyfikacji w danym obszarze.



Rysunek 4. Podstawowy schemat powstawania programu certyfikacji zgodnie z Aktem o Cyberbezpieczeństwie
Źródło: opracowanie własne

Przy ustalaniu priorytetowych obszarów dla programu kroczącego, Komisji doradza Europejska Grupa Certyfikacji Cyberbezpieczeństwa (ECCG), która składa się z przedstawicieli krajowych organów ds. certyfikacji cyberbezpieczeństwa. Mechanizm powstawania programu certyfikacji przedstawiono na Rysunku 4.).

W należycie uzasadnionych przypadkach Komisja może pominąć unijny program kroczący oraz ECCG i bezpośrednio zwrócić się do ENISA o przygotowanie programu certyfikacji. W takim szczególnym trybie, z początkiem 2020 roku rozpoczęły się prace nad wnioskiem Komisji Europejskiej o przygotowanie programu certyfikacji rozwiązań w chmurze[11], który może mieć duże znaczenie dla sektora bankowego. To zagadnienie zostanie szerzej omówione w rozdziale 7.

W europejskich ramach może funkcjonować wiele programów (schematów) certyfikacji cyberbezpieczeństwa, o różnych zakresach przedmiotowych i różnych poziomach uzasadnienia zaufania. Stworzenie europejskich programów oznacza likwidację krajowych programów certyfikacji działających w tym samym zakresie przedmiotowym.

4.2. Zasady działania europejskich ram certyfikacji cyberbezpieczeństwa

Każdy kraj członkowski musi desygnować przynajmniej jedną instytucję odpowiedzialną za certyfikację cyberbezpieczeństwa. Ta instytucja przyznaje akredytacje podmiotom przeprowadzającym ewaluację bezpieczeństwa oraz wydaje certyfikaty. Instytucje krajowe są zobowiązane do ścisłej współpracy ze sobą oraz z ENISA.

W zależności od ryzyka związanego z zamierzonym zastosowaniem, dla przedmiotu oceny zgodności będzie można uzyskać certyfikat cyberbezpieczeństwa na jednym z trzech poziomów uzasadnienia zaufania (assurance level):

- „Podstawowy" (Basic) – certyfikat wydany przez akredytowaną jednostkę oceny zgodności lub deklaracja zgodności, wydawana przez stronę pierwszą, czyli producenta lub dostawcę,
- „Istotny" (Substantial) – certyfikat wydany przez akredytowaną jednostkę oceny zgodności,
- „Wysoki" (High) – certyfikat wydany przez akredytowaną jednostkę oceny zgodności, będącą podmiotem publicznym albo podmiotem prywatnym, na którego delegowano realizację zadania.

[11] https://www.enisa.europa.eu/news/enisa-news/cybersecurity-certification-lifting-the-eu-into-the-cloud dostęp 11.12.2019

Programy certyfikacji muszą być stworzone z uwzględnieniem zasad nadzoru nad rynkiem (normy zharmonizowane – akredytacja jednostek oceniających zgodność) oraz zasad normalizacji (normy i specyfikacje techniczne). Wymagania, jakie musi spełnić europejski program certyfikacji, odnoszą się do następujących zagadnień:

- organizacja programu (struktury),
- wydawanie i utrzymywanie systemu certyfikacji, w tym monitorowanie certyfikatów,
- wymagania w odniesieniu do procesu ewaluacji,
- normy referencyjne,
- własne wewnętrzne wymagania programu (np. w zakresie utrzymania jakości procesów i procedur).

Każdy tak zaprojektowany program, po przejściu procesu przygotowania, konsultowania, opiniowania i akceptacji, w którym swoje role pełni Komisja Europejska, ENISA oraz Kraje Członkowskie (zob. rozdział 5.1), stanie się ogólnoeuropejskim programem certyfikacji cyberbezpieczeństwa.

4.3. System nadzoru nad jednostkami oceny zgodności wydającymi certyfikaty cyberbezpieczeństwa

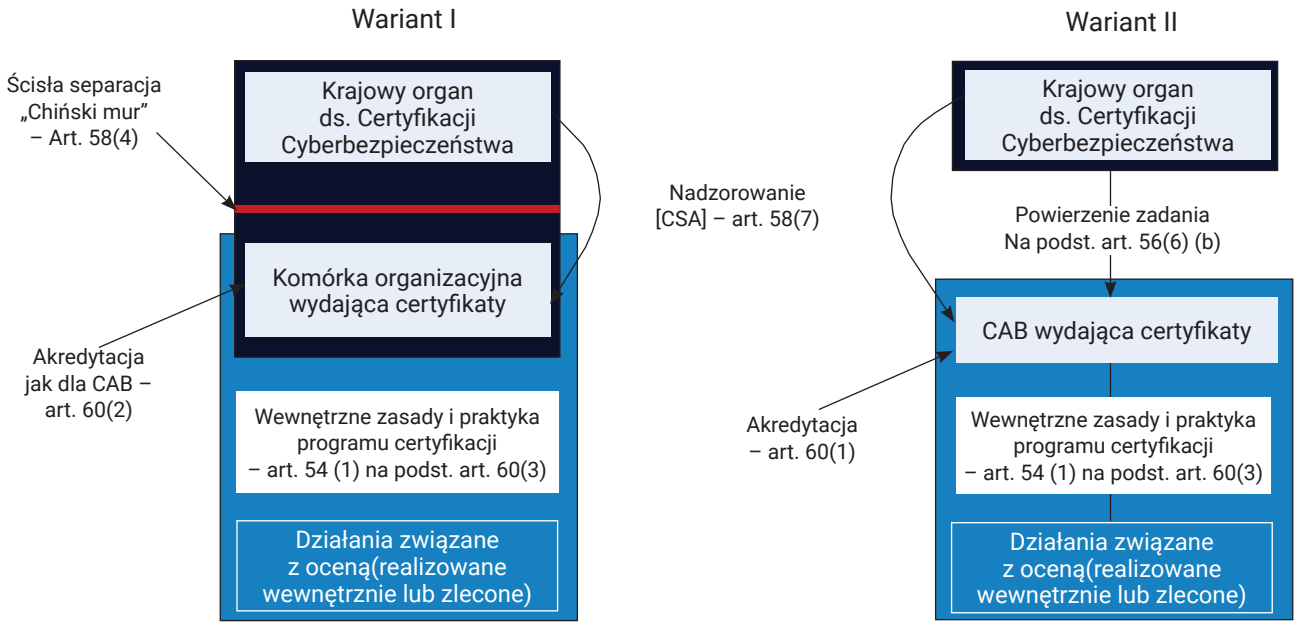
Nadzór nad jednostkami oceny zgodności wydającymi certyfikaty cyberbezpieczeństwa sprawuje krajowy organ, wyznaczony na podstawie przepisów prawa krajowego. Nadzoruje on wykonywanie obowiązków opisanych w CSA przez wszystkich uczestników procesu ewaluacji i certyfikacji oraz współpracuje z organami nadzoru z innych krajów członkowskich UE, Komisją Europejską oraz ENISA. Podstawowym wymogiem dla organu nadzoru jest wymóg bezstronności, możliwy do realizacji w dwóch wariantach (zob. Rysunek 5).

4.4. Aktualny stan wdrożenia systemów certyfikacji w Polsce

Prace nad stworzeniem i wdrożeniem krajowego schematu oceny i certyfikacji cyberbezpieczeństwa rozpoczęły się w 2017 roku, jako projekt finansowany ze środków Narodowego Centrum Badań i Rozwoju w ramach programu krajowego „Cyberbezpieczeństwo i eTożsamość"[12]. Celem projekt KSO3C[13] jest stworzenie struktury organizacyjnej zdolnej do realizacji ocen bezpieczeństw

[12] https://www.ncbr.gov.pl/index.php?id=17259&L=272, dostęp 22.12.2019r.

[13] https://kso3c.pl, dostęp 22.12.2019r.



Rysunek 5. Realizacja zasady niezależności organów nadzoru
Źródło: opracowanie własne

produktów teleinformatycznych i wydawania na ich podstawie certyfikatów, które będą uznawane globalnie. Zakończenie projektu KSO3C i rozpoczęcie świadczenia usług komercyjnych w ramach polskiego schematu jest planowane na koniec lutego 2021.

Wejście w życie Aktu o Cyberbezpieczeństwie i rozpoczęcie pod koniec 2019 roku prac nad wdrożeniem pierwszego europejskiego programu certyfikacji cyberbezpieczeństwa jako następcy SOG-IS objęło także projekt KSO3C – uczestnika porozumienia SOG-IS (zob. też rozdział 6.2).

Od kilkunastu lat funkcjonuje w Polsce certyfikacja systemów zarządzania bezpieczeństwem informacji na zgodność z normą PN EN-ISO/IEC 27001. Na tle innych krajów, liczba certyfikatów wydanych dla organizacji mających siedzibę w Polsce jest duża, i plasuje nasz kraj na początku drugiej dziesiątki w rankingu. O znaczeniu normy EN-ISO/IEC 27001 dla europejskiego programu certyfikacji cyberbezpieczeństwa dla rozwiązań chmurowych będzie jeszcze mowa w rozdziale 6.2.

Ministerstwo Cyfryzacji, jako dział administracji rządowej odpowiedzialny za cyberbezpieczeństwo w Polsce, występuje w charakterze krajowego organu odpowiedzialnego za nadzór nad certyfikacją cyberbezpieczeństwa. Odpowiednie umocowanie ustawowe nastąpi, jak sądzi się powszechnie, przez nowelizację Ustawy o Krajowym Systemie Cyberbezpieczeństwa.

Certyfikacja obowiązkowa a certyfikacja dobrowolna

5.1. Istniejący w UE system oceny zgodności

W odniesieniu do wyrobów, dla których uzyskanie znaku CE jest warunkiem dopuszczenia do obrotu, jednym z typów oceny zgodności jest certyfikacja. Tzw. nowe ramy prawne określają typy produktów, dla których atestacja, że dany produkt spełnia wymagania, jest realizowana przez niezależny podmiot. Dla certyfikacji obowiązkowej są wyznaczone tzw. jednostki notyfikujące, które zapewniają atestację, realizowaną samodzielnie lub za pośrednictwem specjalizowanych laboratoriów oraz wydają odpowiednie certyfikaty poświadczające zgodność z wymaganiami. Wyznaczenie jednostek notyfikujących znajduje się w wyłącznej kompetencji Kraju Członkowskiego. Poza certyfikacją obowiązkową na rynku znajduje miejsce certyfikacja dobrowolna, która jest wyznacznikiem niezależnego potwierdzenia spełnienia wymagań określonych w normach referencyjnych. Certyfikacja dobrowolna może odnosić się do wyrobów, procesów, systemów lub osób.

Niezależnie od tego, czy ocena zgodności ma charakter dobrowolny, czy obowiązkowy, podlega ona systemowi oceny zgodności określonemu w Rozporządzeniu UE 765/2008[14].

W tym Rozporządzeniu określono kompetencje krajowych jednostek akredytujących, sprawujących nadzór nad wszystkimi formami oceny zgodności, a w szczególności nad jednostkami oceniającymi zgodność (*CAB – Conformity Assessment Body*). Odpowiednie, nominowane krajowe jednostki akredytujące zapewniają, że CAB-y mają odpowiedni potencjał techniczny oraz kompetencje, aby przeprowadzić ocenę zgodności w danym obszarze. Krajowa jednostka akredytująca udziela CAB akredytacji w odniesieniu do norm zharmonizowanych, zawierających wymagania dla określonego typu oceny zgodności. Wymagania te zawarte w normach, odpowiednio dla:

– jednostki certyfikującej wyroby – EN-ISO/IEC 17065
– jednostki certyfikującej systemy – EN-ISO/IEC 17021-1
– jednostki certyfikującej osoby – EN ISO/IEC 17024
– laboratoria badawcze, wzorcujące – EN-ISO/IEC 17025

i stanowią podstawę odpowiedniego programu akredytującego dla CAB.

Zgodnie z Rozporządzeniem 765/2008, krajowa jednostka akredytująca jest podmiotem nadzorującym akredytowane CAB-y. Funkcje nadzoru obejmują:

– nadanie CAB – po dokonaniu sprawdzenia – certyfikatu akredytacji,
– monitorowanie zgodności działań CAB z wymaganiami odpowiedniej normy zharmonizowanej przez:
  – audyty nadzoru,
  – system reakcji na skargi i zażalenia na działania CAB,
  – ograniczanie, zawieszanie lub – w skrajnym wypadku – cofnięcie CAB certyfikatu akredytacji.

Krajowe jednostki akredytujące ustanowione w Krajach Członkowskich tworzą wspólną sieć (EA – European Accreditation), której celem jest ujednolicenie praktyk i procedur oraz zapewnienie jakości procesów akredytacji.

5.2. Certyfikacja cyberbezpieczeństwa w CSA pozostała dobrowolna

W trakcie prac nad Aktem o Cyberbezpieczeństwie, najpoważniejszym punktem sporu Rady Europejskiej i Parlamentu Europejskiego była kwestia obowiązkowej certyfikacji cyberbezpieczeństwa. Państwa Członkowskie stały na stanowisku, że certyfikacja ma pozostać dobrowolna, natomiast Parlament Europejski forsował certyfikację obowiązkową w obszarze regulowanym przez Dyrektywę NIS (w odniesieniu do produktów i usług stosowanych przez operatorów usług kluczowych).

Zgodnie z obecnymi zapisami CSA, certyfikacja pozostała co do zasady dobrowolna (z uwzględnieniem przepisów dziedzinowych, w których wskazano obowiązkową certyfikację, np. dotyczącą tachografów czy bezpiecznych urządzeń do składania podpisu elektronicznego lub pieczęci elektronicznej), natomiast wprowadzono mechanizm przeglądu funkcjonującego europejskiego programu certyfikacji cyberbezpieczeństwa pod kątem rozszerzenia zakresu przedmiotowego na produkty/usługi podlegające obowiązkowej certyfikacji, ze szczególnym uwzględnieniem produktów i usług operatorów usług kluczowych, w tym banków. Przegląd ma się odbyć nie wcześniej niż 2 lata po uruchomieniu europejskiego programu certyfikacji cyberbezpieczeństwa i nie później niż w 2023 roku.

Należy wskazać, że obowiązkowa certyfikacja w obszarze świadczenia usług kluczowych dotknie w pierwszym rzędzie sektor bankowy, z uwagi na stosowane zaawansowane rozwiązania teleinformatyczne służące do świadczenia usług bankowych.

[14] https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32008R0765&from=EN, dostęp 22.11.2019r.

Przyszłość certyfikacji cyberbezpieczeństwa – europejskie programy (schematy) certyfikacji cyberbezpieczeństwa

6.1. Role i zadania interesariuszy przy zapewnieniu ładu w systemie certyfikacji cyberbezpieczeństwa

Regularna droga do europejskich programów certyfikacji cyberbezpieczeństwa została opisana jako unijny plan kroczący (tzn. wykaz produktów usług lub procesów ICT, które mają być objęte określonym programem certyfikacji), do którego propozycje mogą zgłaszać wszyscy zainteresowani, w tym kraje członkowskie (działające w formule europejskiej grupy certyfikacji cyberbezpieczeństwa – ECCG), organizacje przedsiębiorców dużych, średnich i małych, przedstawiciele środowisk naukowych oraz normalizacyjnych. Po otrzymaniu propozycji Komisja Europejska zleca ENISA przygotowanie europejskiego programu certyfikacji cyberbezpieczeństwa, wprowadzanego metodą aktu delegowanego.

W zakresie uprawnień Komisji Europejskiej pozostają przeglądy funkcjonowania istniejących programów certyfikacji cyberbezpieczeństwa i podejmowanie odpowiednich działań w celu zwiększenia skuteczności działania takich programów.

6.2. Pierwszy projekt europejskiego programu certyfikacji cyberbezpieczeństwa

Aktualnie trwają prace nad pierwszym projektem zgłoszonym z pominięciem unijnego programu kroczącego (zgodnie z zasadą „w szczególnie uzasadnionych przypadkach"). Projekt jest określany jako „następca SOG-IS". Program certyfikacji ma obejmować produkty ICT oraz profile zabezpieczeń (Protection Profile) i przyznawać certyfikaty na trzech poziomach uzasadnienia zaufania. Program ma przejąć wewnętrzne zasady SOG-IS, o ile te nie są sprzeczne z CSA. Normami referencyjnymi programu będą Common Criteria (CC) oraz Common Evaluation Methodology (CEM). Jako że program znajduje się na etapie projektu, ostateczna postać aktu wykonawczego wdrażającego następcę SOG-IS jako pierwszy europejski program certyfikacji cyberbezpieczeństwa nie jest jeszcze możliwa do przewidzenia. Należy jednakże przyjąć, że zakres przedmiotowy będzie początkowo zbliżony do zakresu produktów, które aktualnie certyfikuje SOG-IS, natomiast z uwagi na znaczenie regulacyjne certyfikacji cyberbezpieczeństwa, podmiotowo obejmie wiele sektorów, w którym SOG-IS był do tej pory dość słabo reprezentowany. W szczególności dotyczy to sektora bankowego (zob. też rozdział Rekomendacji).

Certyfikacja rozwiązań chmurowych

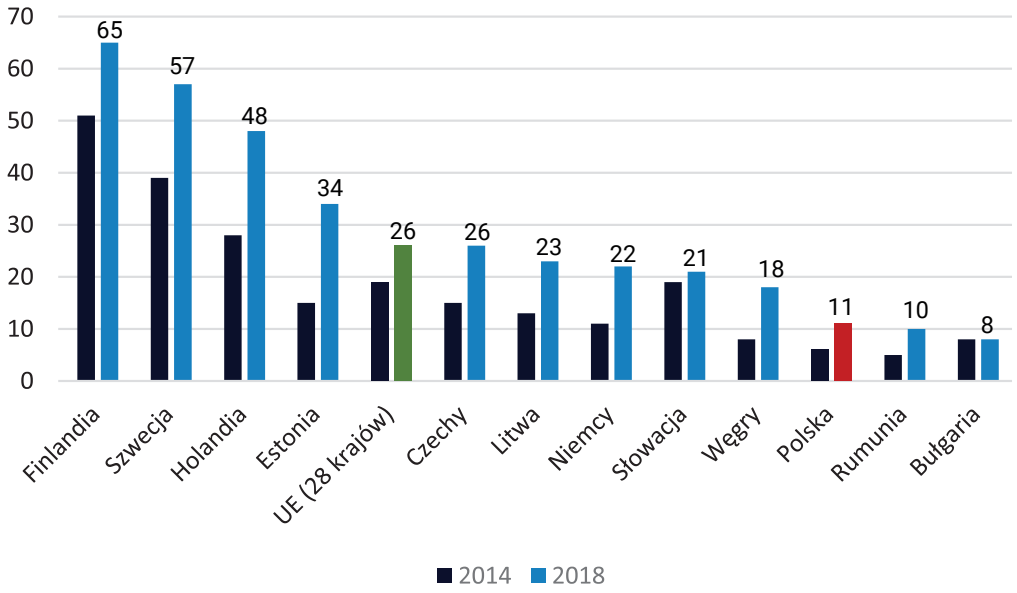
7.1. Wprowadzenie – przekrój zastosowań

Usługi chmury obliczeniowej, czyli udostępnianie miejsca dla przechowywania danych przez usługodawcę klientowi z ciągłym dostępem do tych danych, stają się z roku na rok coraz bardziej popularne.

Chmura obliczeniowa może być wykorzystywana przez przedsiębiorstwa zamiast budowania i utrzymywania własnej infrastruktury IT. Organizacja może wykorzystywać chmurę publiczną (czyli współdzielić przestrzeń z innymi podmiotami) lub chmurę prywatną (gdy infrastruktura jest przypisana wyłącznie do danego przedsiębiorstwa).

Chmura obliczeniowa wciąż jest wykorzystywana jedynie przez niewielką część przedsiębiorstw w Unii Europejskiej. Według badań Eurostatu[15], w 2018 roku 26,2% firm korzystało z usług chmurowych, w porównaniu do 19% w 2014 roku. Należy pamiętać, że w danych Eurostatu uwzględnione są jedynie firmy powyżej 10 pracowników. Między krajami Unii występują znaczące różnice. Przykładowo, w Finlandii aż 65% przedsiębiorstw informuje o korzystaniu z chmury obliczeniowej. Ponad 50% firm wykorzystuje chmurę w Szwecji i Danii. W dolnej części rankingu znajdują się Bułgaria (8%), Rumunia (10%) i Polska (11%). Wybrane kraje przedstawiono na rysunku poniżej (zob. *Rysunek 6).*

Usługi w chmurze mogą spełniać wiele różnych potrzeb przedsiębiorstw. Najwięcej przedsiębiorstw w UE (69%) wykorzystuje chmurę do obsługi poczty elektronicznej. Natomiast tylko 23% wykorzystuje moce obliczeniowe chmury jako podstawę do własnego oprogramowania. W Polsce cele wykorzystania kształtują się podobnie, 67% zastosowań dotyczy poczty elektronicznej, a 15% służy do budowania własnego oprogramowania. Dane o celach wykorzystywania chmury w przedsiębiorstwach w 2018 roku dla wybranych krajów przedstawiono w Tabeli 1 na sąsiedniej stronie.



Rysunek 6. Odsetek przedsiębiorstw wykorzystujących usługi w chmurze w wybranych krajach UE
Źródło: opracowanie własne na postawie danych Eurostat

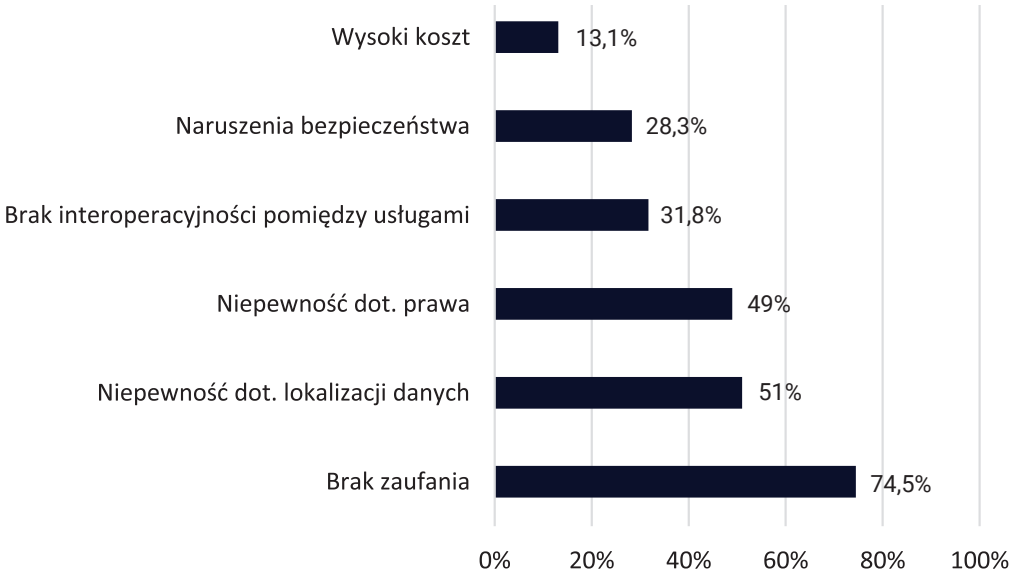
[15] https://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises#Enterprises_using_cloud_computing dostęp 11.12.2019 r.

Tabela 1. Odsetek przedsiębiorstw wykorzystujących rodzaje usług w chmurze w wybranych krajach UE

Kraj	Procent przedsiębiorstw ogółem	E-mail	Przechowywanie plików	Programy biurowe	Hosting baz danych	Programy księgowe lub finansowe	CRM	Moc obliczeniowa dla własnego oprogramowania
Finlandia	65%	79%	69%	65%	53%	56%	37%	18%
Szwecja	57%	72%	74%	53%	52%	51%	31%	26%
Holandia	48%	67%	72%	56%	70%	59%	45%	24%
Estonia	34%	68%	48%	43%	26%	64%	19%	9%
UE (28 krajów)	26%	69%	68%	53%	48%	38%	29%	23%
Czechy	26%	77%	64%	56%	36%	33%	21%	17%
Litwa	23%	70%	61%	39%	52%	41%	27%	36%
Niemcy	22%	48%	61%	34%	33%	28%	19%	19%
Słowacja	21%	83%	60%	60%	39%	44%	26%	25%
Węgry	18%	73%	59%	56%	38%	35%	27%	31%
Polska	11%	67%	53%	51%	33%	27%	23%	15%
Rumunia	10%	77%	60%	52%	50%	50%	0%	31%
Bułgaria	8%	73%	64%	56%	58%	28%	26%	20%

Źródło: opracowanie własne na postawie danych Eurostat

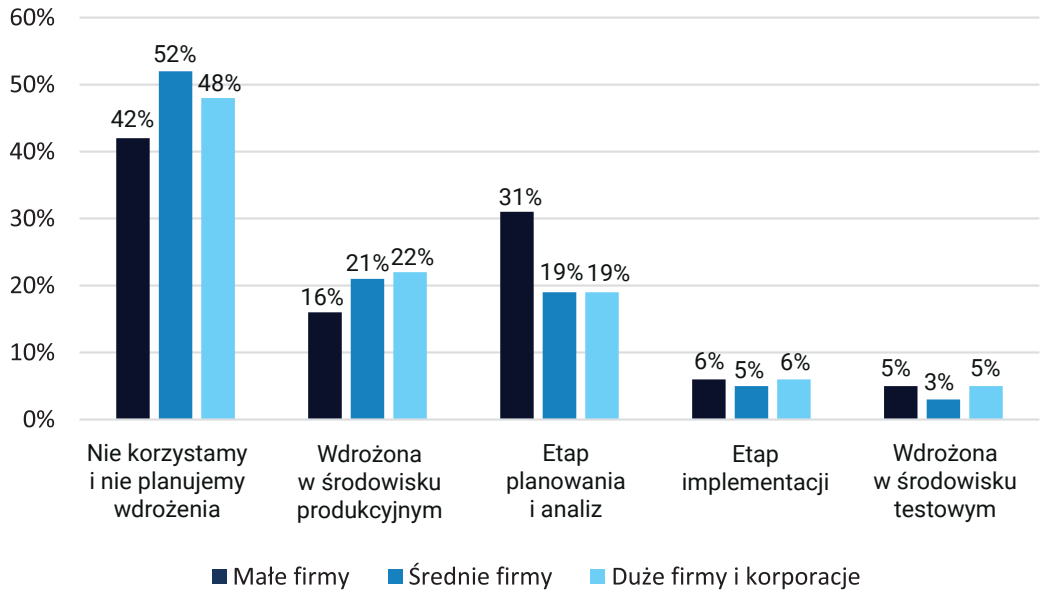
Rysunek 7. Przyczyny braku wykorzystywania usług w chmurze w przedsiębiorstwach UE w 2014 roku
Źródło: opracowanie własne na postawie danych Eurostat



Rysunek 8. Przyczyny braku wykorzystywania usług w chmurze w przedsiębiorstwach UE w 2018 roku
Źródło: opracowanie własne na postawie danych Orue-Echevarria et al.

Największy odsetek przedsiębiorstw wykorzystujących chmurę obliczeniową występuje w sektorze IT i komunikacji (64%), podczas gdy w pozostałych sektorach odsetek oscyluje wokół 20%-30%. Chmura jest również znacznie częściej wykorzystywana w dużych przedsiębiorstwach (56%) niż w małych i średnich (25%).

W roku 2014 zapytano przedsiębiorstwa niekorzystające z usług w chmurze o przyczyny tego stanu rzeczy. Niestety to pytanie nie zostało ponowione w 2018 roku. Jednak nawet z danych z 2014 roku można wyciągnąć kilka wniosków. Najważniejszą przyczyną niechęci do wykorzystywania usług chmurowych są wątpliwości dotyczące bezpieczeństwa danych, zarówno dla dużych, jak i dla małych i średnich przedsiębiorstw. Ponadto duże firmy mają wątpliwości dotyczące prawnych aspektów: jurysdykcji, rozstrzygania sporów oraz miej-



Rysunek 9. Wdrożenia rozwiązań chmurowych w Polsce w 2019 roku w funkcji wielkości firmy
Źródło: opracowanie własne na postawie danych „Chmura publiczna w Polsce 2019"

sca fizycznego przechowywania danych. W małych firmach częściej wymieniane były wysokie koszty kupienia usług w chmurze i niewystarczająca wiedza. Szczegółowe przyczyny przedstawiono na *Rysunku 7* (można było wybrać więcej niż jedną odpowiedź).
W ramach badania ankietowego autorów opracowania dotyczącego certyfikacji w chmurze[16], wykonanego dla Komisji Europejskiej, w 2018 roku najczęściej wymienianym powodem był brak zaufania. Tutaj również można było wybrać więcej niż jedną odpowiedź, co utrudnia jednoznaczną interpretację, do czego zaufania brakuje konsumentom (zob. *Rysunek 8).*

W Polsce stosunek do rozwiązań chmurowych sprawdzano w ramach badania ankietowego „Chmura publiczna w Polsce 2019"[17]. Odpowiedziało 676 przedstawicieli firm różnej wielkości. Pierwsze pytanie dotyczyło stopnia, w jakim przedsiębiorstwa wdrożyły chmurę publiczną (zob. *Rysunek 9).*

Niemal 50% wszystkich ankietowanych stwierdziło, że nie korzystają z chmury i nie planują jej wdrożenia. Tych, którzy korzystają z chmury, zapytano o opinię dotyczącą bezpieczeństwa rozwiązań chmurowych, prosząc o porównanie z sytuacją, gdy dane są przechowywane wewnątrz organizacji (zob. Rysunek 10).

Elementem, który w innych sektorach wpływa pozytywnie na poczucie bezpieczeństwa usługi czy produktu, jest szeroko stosowana i powszechnie znana certyfikacja. Dwie trzecie respondentów w badaniu dla Komisji Europejskiej wyraziło przekonanie, że stworzenie schematu certyfikacji rozwiązań chmurowych będzie miało pozytywny wpływ na poczucie bezpieczeństwa korzystania z usług. W następnej części opracowania omówione zostały najbardziej popularne obecnie dostępne schematy certyfikacji usług chmurowych oraz prace Unii Europejskiej w ramach CSA nad wprowadzeniem wspólnego, jednolitego, unijnego schematu.

7.2. Przegląd istniejących schematów certyfikacji rozwiązań chmurowych – braki i niedostatki

7.2.1. Wstęp

Sposobem na przezwyciężenie wątpliwości użytkowników związanych z bezpieczeństwem danych i zwiększenie poziomu akceptacji rozwiązań chmurowych może być certyfikacja cyberbezpieczeństwa. Istniejące rozwiązania certyfikacyjne charakteryzują się znacznym rozproszeniem, zarówno na poziomie globalnym, jak i krajowym oraz niejasnością w odniesieniu do stosowanych norm refe-

[16] „Certification Schemes for Cloud Computing", Orue-Echevarria et al., European Union 2018
[17] https://www.cloudforum.pl/wp-content/uploads/2019/05/Raport-Chmura-publiczna-w-Polsce-2019_CZ.-1_POZIOM-ADAPTACJI-US%C5%81UG-CHMURY-PUBLICZNEJ_IDG_Oktawave.pdf, dostęp 1.12.2019

Rysunek 10. Bezpieczeństwo przechowywania danych w chmurze
Źródło: opracowanie własne na postawie danych „Chmura Publiczna w Polsce 2019"

rencyjnych do oceny zgodności. Dodatkowo wiele krajów wypracowało własne rozwiązania, których przestrzegania wymaga od chmur obliczeniowych działających na ich terytorium. Ogólnie w ramach raportu KE dot. Certyfikacji rozwiązań chmurowych, zidentyfikowano ponad 20 różnych programów certyfikacji. Najczęściej wykorzystywanym programem certyfikacji jest ISO 27001, następnie CSA Star, PCI-DSS i seria SOC.

7.2.2. Normy międzynarodowe

EN – ISO/IEC 27001 jest najczęściej wykorzystywaną normą dotyczącą systemów zarządzania bezpieczeństwem informacji w wielu sektorach i nie obejmuje specyfiki rozwiązań chmurowych. Wstępnie opisana została w części 2.4 niniejszego opracowania. Szczegółowe omówienie normy znajduje się w załączniku A.

7.2.3. Standardy branżowe

ISAE 3402 – SOC 1, SOC 2, SOC3[18]
Są to standardy związane z audytem i poświadczeniem jakości dostarczanej usługi, niespecyficzne dla sektora rozwiązań chmurowych. Amerykański Instytut Certyfikowanych Księgowych (AICPA) określa trzy rodzaje raportów audytowych, które mogą być przekazane przez dostawcę usług klientowi, w celu udowodnienia jakości swoich zabezpieczeń:

SOC1 (Service Organization Control) dotyczy głównie zabezpieczeń wewnątrz organizacji mających wpływ na sprawozdanie finansowe. W Polsce najbardziej popularne jest przeprowadzenie audytu w oparciu o standard ISAE 3402, część międzynarodowych standardów audytu. Istnieją dwa rodzaje raportu audytowego wg **ISAE 3402**:

- typ I dotyczy opisu systemu i ocenę konstrukcji wewnętrznych procedur kontrolnych
- typ II to dodatkowo ocena rzeczywistej skuteczności wewnętrznych procedur

SOC2 dotyczy procesów niewpływających na sprawozdanie finansowe, ale mających znaczenie dla jakości dostarczonej usługi, przede wszystkim procesów IT. Skupia się na Trust Services Principles – security (bezpieczeństwo), availability (dostępność), processing integrity (integralność przetwarzania), confidentiality (poufność) oraz privacy (prywatność). Zakres raportu zwykle różni się pomiędzy usługodawcami, którzy przechodzą audyt, by potwierdzić jakość zabezpieczeń w procesach istotnych dla świadczonej usługi. Ze względu na szczegółowość i wrażliwość informacji w nim zawartej, jedynie informacja o pomyślnym przebyciu audytu zostaje upubliczniona.

SOC3 również opiera się na Trust Services Principles, lecz zawiera ograniczoną ilość informacji w stosunku

[18] https://isae3402.co.uk/isae-3402, dostęp 1.12.2019 r.

do SOC2 i może być udostępniany również publicznie. Zawiera potwierdzenie pomyślnego przejścia audytu oraz zapewnienie władz spółki o spełnieniu wymagań. Często zatem jest wykorzystywany w celach marketingowych.

Firma legitymująca się raportem SOC ma potwierdzoną skuteczność kontroli wewnętrznych w firmie. W kontekście rozwiązań chmurowych, często klient wymaga raportu SOC przed powierzeniem firmie swoich danych.

CSA (Cloud Security Alliance Cloud Control Matrix)[19]
CSA CCM to ramy zabezpieczeń rozwiązań chmurowych, składające się ze 133 zabezpieczeń pogrupowanych w 16 obszarów. Mogą być wykorzystane do systematycznej oceny bezpieczeństwa, natomiast nie są standardem kończącym się certyfikacją. Ramy są silnie osadzone w specyfice rozwiązań chmurowych, kładąc duży nacisk na podział zabezpieczeń i odpowiedzialności pomiędzy podmiotami uczestniczącymi w łańcuchu dostaw. Odnoszą się do szerokiego zakresu zagadnień: bezpieczeństwa aplikacji, zarządzania dostępem, bezpieczeństwa rozwiązań mobilnych, kryptografii.

CSA STAR Attestation[20] oparte jest na przejściu audytu SOC1 albo SOC2 połączonego z oceną na podstawie CSA CCM. Warunkiem otrzymania certyfikatu CSA STAR jest posiadanie certyfikatu zgodności systemu zarządzania bezpieczeństwem informacji z EN – ISO/IEC 27001. Certyfikat jest wydawany na trzy lata, z coroczną re-ewaluacją. Gdy organizacja próbuje zdobyć jednocześnie certyfikat na zgodność z EN – ISO/IEC 27001 i CSA CCM, musi przejść ewaluację dwustopniową – najpierw na EN – ISO/IEC 27001, a potem na zabezpieczenia zgodne z CSA CCM. W wypadku, gdy organizacja posiada już certyfikat zgodności z EN – ISO/IEC 27001, to jedynie dodatkowe zabezpieczenia z CCM stanowią przedmiot ewaluacji.

7.2.4. Normy krajowe w ramach UE

BSI Cloud Computing Compliance Controls Catalog C5 (Niemcy)[21]
BSI C5 to standard bezpieczeństwa danych w chmurze użytkowanej przez rząd niemiecki. Obejmuje zabezpieczenia z EN – ISO/IEC 27001, CSA CCM, AICPA Trust Service Principle oraz niemieckie zasady bezpieczeństwa IT. Podejście zostało opracowane we współpracy z francuską agencją ds. cyberbezpieczeństwa ANSSI, która opracowała analogiczny standard francuski (SecNumCloud, zob. niżej). Raport stwierdzający zgodność z BSI C5 jest analogiczny do raportu zgodności z ISAE 3402 i SOC2. Jest to certyfikat dla dostawców usług w chmurze, potwierdzający bezpieczeństwo i transparentność. Oparcie standardu na ISAE 3402 I SOC2 pozwala na wykonanie audytu na zgodność z BSI C5 przez tych samych certyfikowanych audytorów, w ramach tej samej ewaluacji.

ANSII SecNumCloud (Francja)[22]
ANSII jest francuską agencją rządową odpowiedzialną za bezpieczeństwo i ochronę systemów informatycznych. Standard SecNumCloud powstał w 2016 roku i jest częścią podejścia ANSII wydawania „Wiz bezpieczeństwa", dla produktów spełniających wymagania. Zgodność ze standardem poddawana jest ewaluacji, wykonywanej w uznanych przez Agencję laboratoriach. Został on opracowany we współpracy z niemiecką agencją BSI.

ASIP HDS Personal Health Data Protection (Francja)[23]
Certyfikat HDS ma na celu wzmocnienie ochrony danych o stanie zdrowia osoby. Jest to certyfikat wydany przez francuską agencję rządową ds. cyfryzacji służby zdrowia. Posiadanie certyfikatu umożliwia przechowywanie danych francuskich pacjentów w chmurze. Dostawca usług w chmurze może uzyskać certyfikat w dwóch obszarach:

– usługodawcy dostarczającego infrastrukturę fizyczną (zapewnienie i utrzymanie miejsc fizycznych do obsługi infrastruktury systemu informatycznego, wykorzystywanego do przetwarzania danych o zdrowiu);
– dostawy hostingu (zapewnienie i utrzymanie platformy będącej hostem dla aplikacji systemu; zapewnienie i utrzymanie wirtualnej infrastruktury systemu informatycznego wykorzystywanego do przetwarzania danych o zdrowiu, outsourcing kopii zapasowych danych o zdrowiu).

Esquema Nacional de Seguridad (ENS)/ High Spanish Government Standards (Hiszpania)
ENS to hiszpański schemat certyfikacji, stworzony w Ministerstwie Finansów oraz w Narodowym Centrum Kryptologii (CCN). Zgodność z ENS wymagana jest od wszystkich agencji rządowych i organizacji publicznych, a także dostawców usług wykorzystywanych w ramach usług publicznych. Otrzymanie certyfikatu wymaga przejścia audytu, wykonanego przez niezależnego, akredytowanego audytora.

[19] https://cloudsecurityalliance.org/research/working-groups/cloud-controls-matrix/, dostęp 10.12.2019 r.
[20] https://cloudsecurityalliance.org/star/, dostęp 10.12.2019 r.
[21] https://www.bsi.bund.de/EN/Topics/CloudComputing/Compliance_Controls_Catalogue/Compliance_Controls_Catalogue_node.html, dostęp 10.12.2019 r.
[22] https://www.ssi.gouv.fr/actualite/secnumcloud-evolue-et-passe-a-lheure-du-rgpd/ , dostęp 10.12.2019 r.
[23] https://esante.gouv.fr/labels-certifications/hds/certification-des-hebergeurs-de-donnees-de-sante dostęp 1.12.2019

Cyber Essentials Plus Cyber Threat Protection (Wielka Brytania)[24]
Cyber Essentials Plus to standard brytyjski, wprowadzony w celu potwierdzenia ochrony przed najczęstszymi cyberatakami. To zestaw zabezpieczeń technicznych, z którymi zgodność sprawdzana jest corocznie przez akredytowanego, niezależnego audytora.

G-Cloud Government Standard (Wielka Brytania)[25]
Standard brytyjski, wspierany przez rząd, pozwalający certyfikowanym podmiotom brać udział w programie rządowym przejścia usług rządowych na rozwiązania chmurowe „Cloud First". Certyfikowany dostawca usług chmurowych może sprzedawać swoje usługi podmiotom publicznym w ramach krótkoterminowych, szybkich zakupów z wolnej ręki.

7.3. Prace przygotowawcze do europejskiej certyfikacji rozwiązań chmurowych

W ramach strategii Jednolitego Rynku Cyfrowego, Komisja Europejska prowadzi prace nad wprowadzeniem europejskiego programu certyfikacji rozwiązań chmurowych.

W ramach grupy roboczej CSP CERT, powstały zalecenia, jak taka certyfikacja miałaby wyglądać, przy uwzględnieniu wymagań CSA. Opracowano propozycję Cloud Computing Assurance Levels (CCAL), względem których prowadzona będzie certyfikacja. CSP CERT nie rekomenduje opracowania całkowicie nowego programu certyfikacji, tylko wykorzystanie rozwiązań bazujących na istniejących praktykach/ schematach/ standardach. Rekomendowane jest włączenie prac nad programem certyfikacji rozwiązań chmurowych do unijnego programu kroczącego certyfikacji cyberbezpieczeństwa w ramach CSA oraz zlecenie ENISA przygotowania propozycji programu certyfikacji na podstawie istniejących rozwiązań.

Zgodnie z informacjami prasowymi na początku grudnia 2019 roku Komisja Europejska zgłosiła projekt europejskiego programu certyfikacji cyberbezpieczeństwa w obszarze przetwarzania chmurowego, do dalszego przygotowania przez ENISA.

7.4. Wpływ certyfikacji na zastosowanie rozwiązań chmurowych w sektorze bankowym

Rozwiązania chmurowe w sektorze bankowym mają ogromny potencjał. Wykorzystanie możliwości obliczeniowych chmury pozwala np. na wdrożenie systemów marketingowych opartych na sztucznej inteligencji. Jednakże, ze względów bezpieczeństwa regulator (KNF) mocno ogranicza obecnie możliwości wykorzystania usług zewnętrznych, w tym chmurowych. Dane przetwarzane przez banki są również niezwykle wrażliwe i ich przekazywanie podmiotom zewnętrznym podlega przepisom prawa dotyczącym ochrony danych osobowych. Certyfikacja bezpieczeństwa rozwiązań chmurowych wprowadza zewnętrzne, niezależne potwierdzenie bezpieczeństwa. Wraz ze wzrostem istotności certyfikacji oraz promowaniem jej przez Unię Europejską pojawi się presja na regulatora, by uelastycznić reguły wykorzystywania certyfikowanych usług. Certyfikacja wpłynie także na chęć wykorzystywania rozwiązań chmurowych przez przedsiębiorstwa, w tym funkcjonujące w sektorze bankowym, co przyspieszy rozwój technologii, a tym samym zwiększy jej znaczenie oraz możliwości zastosowania.

[24] https://www.cyberessentials.ncsc.gov.uk/ dostęp 2.12.2019
[25] https://www.digitalmarketplace.service.gov.uk/ dostęp 2.12.2019

Rekomendacje dalszych działań

Rekomendacje dla banków

Rekomendacja 1. W najbliższych latach (do 2023 r.) należy przewidywać wprowadzenie obowiązkowej certyfikacji cyberbezpieczeństwa produktów i usług związanych ze świadczeniem usług przez operatorów usług kluczowych, do których – zgodnie z Dyrektywą NIS oraz Ustawą o Krajowym Systemie Cyberbezpieczeństwa – zalicza się bankowość i infrastrukturę rynków finansowych.

Rekomendacja 2. Z uwagi na wieloletnie horyzonty inwestycji, planowanie nowych rozwiązań należy już dziś odnosić do możliwości zastosowania certyfikowanych produktów lub usług. Pożądanym działaniem powinno być nadanie priorytetów dla prac badawczo-rozwojowych, których cele są związane z oceną zgodności i certyfikacją (obejmuje to m.in. specyficzny sposób przygotowywania dokumentacji rozwiązania teleinformatycznego – produktu lub usługi). Należy także rozważyć określenie zespołom bądź pracownikom zadań związanych z monitorowaniem aktywności legislacyjnej w Unii Europejskiej oraz regulacyjnej KNF w zakresie certyfikacji produktów i usług, które mogą mieć zastosowanie w systemach bankowych. Ze szczególnym zainteresowaniem banków powinny spotkać się pierwsze dwa europejskie programy certyfikacji cyberbezpieczeństwa, tzn. a) „następca" SOG-IS oraz b) CCAL. Z planów Komisji Europejskiej wynika, że aktu delegowanego dot. następcy SOG-IS należy spodziewać się pod koniec II kwartału 2020 r. Dla drugiego programu Komisja jeszcze nie określiła harmonogramu działań. Europejskie programy certyfikacji cyberbezpieczeństwa mogą mieć duże znaczenie dla rynków regulowanych, takich jak sektor bankowy. W szczególności, certyfikacja usług chmurowych może pomóc zniwelować ostrożność Komisji Nadzoru Finansowego wyrażaną w odniesieniu do tej formy outsourcingu.

Rekomendacja 3. W kontekście dominacji globalnych schematów certyfikacji dla produktów i usług bankowych (tzn. EMVCo i PCI SSC) należy wskazać, że tego typu schematy znajdują się poza zakresem CSA albo poziom uzasadnienia zaufania do takich certyfikatów będzie ograniczony maksymalnie do 'istotnego'.

Jednakże zgodnie z CSA, certyfikaty z uzasadnieniem zaufania 'wysoki' mogą być wydawane wyłącznie przez jednostki certyfikujące, które są podmiotami publicznymi, którymi te organizacje nie są. Ponadto, globalne schematy certyfikacji nie są budowane w rygorze systemu oceny zgodności opartego na normach zharmonizowanych.

Banki, jako instytucje zaufania publicznego i operatorzy usług kluczowych, będą potrzebować certyfikacji zgodnej z CSA, na poziomie uzasadnienia zaufania 'wysoki'. Należy przyjąć, że pierwsze europejskie programy certyfikacji cyberbezpieczeństwa (w szczególności „następca" SOG-IS) – z uwagi na najbardziej zaawansowane metodyki ewaluacji – będą oferować certyfikację na poziomie uzasadnienia zaufania 'wysoki'.

W tym kontekście należy wskazać na inicjatywę europejską w ramach SEPA Card Framework i opracowane profile zabezpieczeń dla terminali płatniczych jako dobry punkt startowy do dalszego rozwoju.

Rekomendacja 4. Polityka Unii Europejskiej Wspólnego Rynku Cyfrowego promuje rozwiązania chmurowe. Jednym z pierwszych obszarów certyfikacji europejskiej pod CSA ma być właśnie chmura. Jako że rozwiązania w NIS oraz CSA odnoszą się do swobodnego przepływu danych nieosobowych, kwestią otwartą pozostaje, jak odniosą się do np. danych klientów banków. Przepływ danych osobowych regulowany jest przez RODO. Rozwiązania łączące oba typy danych będą w najbliższych latach przedmiotem dyskusji i warto, aby odpowiednie organizacje sektora bankowego, w tym w Polsce, monitorowały postęp prac np. w postaci dedykowanych zespołów roboczych oraz aktywnie wspierały lub wręcz inicjowały rozwiązania korzystne dla sektora.

Rekomendacja 5. Nowe rozwiązania chmurowe w sektorze bankowym powinny być projektowane z uwzględnieniem możliwości certyfikacji w europejskim programie certyfikacji cyberbezpieczeństwa.

Rekomendacja 6. Dyrektywa PSD2 wprowadza nowy rodzaj usługodawców na rynku finansowym – Third Party Providers (TPP). Obowiązek udzielenia dostępu do danych klientów banków takim podmiotom wprowadza zagrożenie na styku systemów banku oraz usługodawcy. Certyfikacja platform współpracy z zewnętrznymi podmiotami lub interfejsów służących do zapewnienia przepływów danych stanowić będzie potwierdzenie bezpieczeństwa w tym punkcie, zarówno w oczach Regulatora, kontrahentów, jak i konsumentów. Zgodnie z przepisami Aktu o Cyberbezpieczeństwie, istnieje możliwość powołania do życia laboratorium ewaluacyjnego przez sektor bankowy, uwzględniającego specyfikę sektora i realizującego usługi ewaluacji produktów i usług w określonym programie certyfikacji cyberbezpieczeństwa. Takie laboratorium musi otrzymać akredytację z Polskiego Centrum Akredytacji, gdzie jednym z kryteriów jest potwierdzenie niezależności, a efekty jego ewaluacji podlegają również monitorowaniu ze strony jednostki certyfikacyjnej.

Rekomendacje dla Regulatora

Rekomendacja 7. W związku z silną presją regulacyjną UE dotyczącą usług kluczowych, kwestia cyberbezpieczeństwa powinna pojawić się w rozwiązaniach regulatora z odpowiednim priorytetem. W szczególności, kwestie niedostatecznej współpracy z podmiotami zewnętrznymi w zakresie raportowania i przeciwdziałania incydentom mogą stanowić potencjalną słabość bankowego systemu ochrony informacji i z tego względu powinny być przedmiotem działań KNF.

Rekomendacja 8. Rozwój technologiczny rozwiązań chmurowych będzie powodował coraz większą presję na umożliwienie bankom szerszego korzystania z usług outsourcingu w tej formule. Wymóg certyfikacji bezpieczeństwa rozwiązań chmurowych może być dobrym zabezpieczeniem, pozwalającym na uelastycznienie regulacji dotyczących outsourcingu.

Rekomendacje dla Ministerstwa Cyfryzacji

Rekomendacja 9. Wprowadzenie przez Unię Europejską koncepcji certyfikacji cyberbezpieczeństwa może oznaczać zupełnie nową jakość produktów i usług funkcjonujących w ramach Jednolitego Rynku Cyfrowego. Do tej pory dobrowolna i specyficzna dla niektórych sektorów certyfikacja pojawi się w wielu dziedzinach życia i niechybnie dosięgnie też sektora bankowego. Można spodziewać się w dalszych krokach np. obowiązku certyfikacji bezpieczeństwa aplikacji mobilnych. Należy spodziewać się dalszego doprecyzowania zakresu Dyrektywy NIS, rozszerzenia wymagań bezpieczeństwa dla operatorów kluczowych oraz silniejszego powiązania zmienionej Dyrektywy z Aktem o Cyberbezpieczeństwie. Z tego względu należy myśleć o zorganizowanej, silnej grupie interesariuszy, w tym też osób z sektora bankowego, którzy mogą wspierać merytorycznie działania przedstawicieli rządu, aby przyszłe rozwiązania były korzystne i dla Polski, i dla sektora bankowego w Polsce.

Rekomendacja 10. Certyfikacja cyberbezpieczeństwa nie zaistniała do tej pory w świadomości konsumentów i przedsiębiorców jako znaczący wyróżnik jakości i zaufania, tak jak chociażby atesty bezpieczeństwa użytkowania produktów (znak CE). Wraz z pojawieniem się unijnych certyfikatów cyberbezpieczeństwa ich zasięg oraz marka instytucji za nimi stojącej może zmienić ten stan rzeczy. Można się również spodziewać inicjatyw podszywających się pod certyfikaty unijne. Edukacja w zakresie rozpoznawania prawdziwej certyfikacji wiąże się z ochroną konsumentów na rynku cyfrowym i powinna znaleźć się w gestii Ministerstwa Cyfryzacji.

Przegląd normy EN – ISO/IEC 27001

A.1. Wprowadzenie

Norma ISO/IEC 27001z ostała przyjęta jako podstawa oceny zgodności dla systemów zarządzania bezpieczeństwem informacji przez *International Accreditation Forum* (IAF) oraz, w konsekwencji, przez jednostki akredytacyjne poszczególnych krajów (w Polsce – przez Polskie Centrum Akredytacji).

W 2013 roku zakończono prace nad nowym wydaniem normy ISO/IEC 27001, a w grudniu 2014 roku została opublikowana PN-ISO/IEC 27001:2014.

Nowe wydanie normy ISO/IEC 27001 zostało przygotowane zgodnie z zatwierdzonym przez ISO nowym podejściem do norm systemów zarządzania.

A.2. Opis wymagań dla systemu zarządzania bezpieczeństwem informacji

Z pierwszego rozdziału normy dotyczącego wymagań (4. Kontekst organizacji) wynika, że organizacja powinna umieć opisać charakter i specyfikę swojej działalności, zidentyfikować swoje procesy biznesowe, określić zakres i stopień uzależnienia od dostawców lub klientów. Ponadto, analiza powinna obejmować potrzeby i wymagania, które są formułowane przez zainteresowane strony. W ten sposób organizacja może zdefiniować cele, wymagania, zakres oraz granice systemu zarządzania. Wymagania opisane w tym rozdziale nie zależą od specyfiki systemu zarządzania i w związku z tym nie ma potrzeby ich rozszerzenia o kwestie związane z bezpieczeństwem informacji.

W kolejnym rozdziale (5. Przywództwo) znajdują się wymagania w odniesieniu nie tylko do zarządzania, ale także do obszaru przywództwa. W tym sensie w tym rozdziale można zidentyfikować wymagania odnoszące się do nadzoru (*governance*) w systemie zarządzania, w tym wytyczania kierunków i zatwierdzania polityki, monitorowania i oceny wyników, a także stwarzania warunków do ciągłego doskonalenia systemu zarządzania. Ponadto, wymagania opisane w tym rozdziale odnoszą się do podziału ról i odpowiedzialności oraz zapewnienia zasobów. Tak, jak poprzednio, wymagania zawarte w tym rozdziale nie zależą od specyfiki systemu zarządzania.

Następny rozdział (6. Planowanie) jest konsekwencją opisu kontekstu i efektów uzyskanych na skutek spełnienia wymagań zawartych w rozdziale 4. Normy. Na etapie planowania przedmiotem analizy jest ryzyko rozumiane jako niepewność osiągnięcia celów bezpieczeństwa informacji. Planowanie obejmuje rozpisanie, jak, kto, kiedy i za ile będzie realizował przedsięwzięcia nakierowane na osiągnięcie celów i ciągłe doskonalenie, optymalizując ryzyka i wykorzystując szanse.

W tym rozdziale wymagania zostały istotnie rozszerzone o elementy związane z szacowaniem i postępowaniem z ryzykiem związanym z bezpieczeństwem informacji. Na tym etapie zostały wskazane wymagania polegające na określeniu kryteriów związanych z procesem szacowania ryzyka oraz akceptowania ryzyka. Wymagania w tej części obejmują także wybór zabezpieczeń i planowanie działań w celu ograniczania ryzyka specyficznego dla bezpieczeństwa informacji, z wykorzystaniem celów stosowania zabezpieczeń oraz zabezpieczeń, których lista znajduje się w Załączniku A normy ISO/IEC 27001.

Wymagania opisane w kolejnym rozdziale (7.Wsparcie) to cała sfera działań zapewniających możliwość poprawnego funkcjonowania systemu zarządzania, począwszy od wymagań dotyczących potrzebnych zasobów, przez wiedzę, umiejętności i doświadczenia osób realizujących procesy systemu zarządzania, programy uświadamiania, procesy komunikacji oraz procesy zarządzania udokumentowanymi informacjami. W tej części normy także nie ma wymagań specyficznych dla obszaru bezpieczeństwa informacji.

W kolejnym rozdziale (8. Działania operacyjne) wymagania ogólne koncentrują się na szczegółowym (w ujęciu projektowym) planowaniu, wdrożeniu oraz nadzorze nad działaniami służącymi spełnieniu celów bezpieczeństwa informacji (zob. rozdział 6). Szczególnie w tym rozdziale były przewidziane rozszerzenia specyficzne dla danego obszaru, którego dotyczy system zarządzania. W wypadku ISO/IEC 27001 kolejne wymagania dotyczą konkretnych realizacji procesu szacowania, a następnie postępowania z ryzykiem, np. w ramach procedur zarządzania zmianami.

Następny rozdział (9. Ocena wyników) zawiera wymagania odnoszące się do uzyskiwania wiarygodnych informacji o funkcjonowaniu systemu zarządzania. Te z kolei dotyczą trzech różnych obszarów:

a) pierwszy podrozdział (9.1) zawiera wymagania dotyczące procesów monitorowania, pomiaru, analizy i oceny wyników systemu zarządzania, w tym wymagania w stosunku do zakresu monitorowania lub pomiaru (dotyczą zarówno systemu zarządzania, jak i zabezpieczeń), a także zastosowanych metod, które powinny zapewniać porównywalne i powtarzalne wyniki,
b) następny podrozdział (9.2) dotyczy organizacji oraz trybu przeprowadzania audytów wewnętrznych systemu zarządzania,

c) ostatni podrozdział (9.3) odnosi się do wymagań przeglądu zarządzania, realizowanego przez kierownictwo organizacji, których spełnienie powinno dać odpowiedź na pytanie o przydatność, adekwatność i skuteczność systemu zarządzania.

Wreszcie ostatni rozdział (10. Doskonalenie) obejmuje wymagania odnoszące się do dwóch zagadnień:

a) zdolności systemu zarządzania do identyfikowania niezgodności, a następnie zapewnienia skutecznych metod analizy oraz reakcji na wystąpienie niezgodności, a także działań korygujących mających na celu usunięcie przyczyny niezgodności (podrozdział 10.1).
b) zapewnienia stałego doskonalenia procesów, mechanizmów oraz struktur systemu zarządzania.