PROCES CERTYFIKACJI SYSTEMÓW INSTYTUCJI FINANSOWYCH – WNIOSKI DLA SEKTORA BANKOWEGO

PROF. DR HAB. MIROSŁAW KUTYŁOWSKI
DR INŻ. ANNA LAUKS-DUTKA

SYGN. WIB PAB 2020/2

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

Wrocław, 09.02.2020

PROGRAM ANALITYCZNO BADAWCZY

Autorzy:

Prof. dr hab. Mirosław Kutyłowski – profesor w Katedrze Podstaw Informatyki Politechniki Wrocławskiej. W przeszłości Huboldt Fellow na Uniwersytecie Technicznym w Darmstadt, docent w Heinz-Nixdorf Institut. Niedawno otrzymał tytuł Hua Shan Professor na uniwersytecie Xidian w ChRL. Członek z wyboru Centralnej Komisji ds. Stopni i Tytułów Naukowych. Obecnie zajmuje się głównie aspektami bezpieczeństwa komputerowego w kontekście protokołów kryptograficznych i ochrony prywatności. Szczególną uwagę poświęca zagadnieniom technicznej realizacji ochrony danych osobowych i protokołom eID.

Dr inż. Anna Lauks-Dutka – wykładowca akademicki w Katedrze Podstaw Informatyki Politechniki Wrocławskiej. Stopień doktora nauk matematycznych w zakresie informatyki uzyskała w IPI PAN. Jej zainteresowania badawcze skupiają się wokół protokołów zapewniających anonimowość, podpisów cyfrowych, bezpieczeństwa informacji oraz prawnych aspektów komunikacji elektronicznej.

Spis treści

Wstęp

Certyfikacja systemów IT, choć nie jest jeszcze dla sektora bankowego narzucona literą prawa, powinna nabierać coraz większego znaczenia jako efektywne narzędzie podnoszące poziom cyberbezpieczeństwa. Podejmując decyzję na temat zastosowania certyfikacji systemów, należy mieć na uwadze:

- rzeczywisty efekt postępowań certyfikacyjnych - trzeba mieć świadomość tego, w czym certyfikacja bezpieczeństwa może być pomocna oraz jakie ograniczenia są związane z procedurami certyfikacyjnymi; niewłaściwie postawione wymagania podlegające certyfikacji lub niewłaściwa interpretacja wyników mogą w konsekwencji istotnie wpłynąć na realny poziom bezpieczeństwa,
- dostępność schematów certyfikacji adekwatnych lub łatwych do zaadoptowania w kontekście zastosowań w sektorze finansowym,
- kierunek zmian legislacyjnych i działania w kierunku europejskiego systemu certyfikacji.

Niniejsza opinia prezentuje rekomendacje autorów wynikające z ich doświadczenia w zakresie prowadzonych prac naukowych w obszarze cyberbezpieczeństwa.

Najważniejsze aspekty procesów certyfikacji w kontekście sektora bankowego

W niniejszym rozdziale przypominamy w syntetycznym skrócie najważniejsze cechy procedur certyfikacyjnych – zarówno ich mocne, jak i słabe strony.

2.1. Korzyści wynikające z poddania się procedurom certyfikacji

Poddanie się procesowi certyfikacji może prowadzić do **ujawnienia szeregu krytycznych problemów w zakresie cyberbezpieczeństwa**. Przykładami takich problemów są:

- **Pominięcie w analizie ryzyka pewnych istotnych zagrożeń.** Zjawisko to występuje również w przypadku systemów budowanych przez bardzo kompetentne zespoły, w istocie posiadające wiedzę i kompetencje w zakresie pominiętych zagrożeń. **"Zapomnienie" o niektórych aspektach jest normalnym zjawiskiem obserwowanym powszechnie**, również w najlepszych zespołach.

- **Brak komponentów będących odpowiedzią na zidentyfikowane zagrożenia.** Częstym źródłem problemów w cyberbezpieczeństwie jest podział na zespoły odpowiadające za różne aspekty. Zespoły mogą działać bezbłędnie, jednak nieporozumienia mogą powstawać na styku zespołów.

- **Wykorzystanie rozwiązań przeznaczonych do innych zastosowań.** Pochopnie mogą być stosowane komponenty, których specyfikacja tylko z pozoru odpowiada potrzebom. Zidentyfikowanie błędu wymagałoby głębszej wiedzy na temat komponentu, trudnej do uzyskania w ramach zwykłego procesu decyzyjnego.

- **Pozostawienie "zapadek" w systemie ułatwiających prace administracyjne, ale zarazem stanowiące o podatności systemu.** Osoby odpowiadające za bieżące administrowanie systemem, a przeciążone zadaniami, mogą wprowadzać ułatwienia, które w konsekwencji mogą prowadzić do osłabienia odporności całego systemu. Certyfikacja powinna wymusić podział ról w sytuacji konfliktu interesów.

Niezwykle pozytywnym efektem certyfikacji jest:

- **Wyeliminowanie niebezpieczeństwa budowy słabo wyspecyfikowanego systemu lub systemu, w którym istotne obszary nie zostały prawidłowo udokumentowane**. Certyfikacja wymusza opracowanie szeregu dokumentów na potrzeby samego procesu. Jakkolwiek jest to uciążliwe i samo w sobie nie stanowi o polepszeniu jakości systemu, pozwala jednak ujawnić obszary, w których nie zachowano należytej staranności i zrealizowano jedynie prowizoryczne rozwiązania. Wykonawcy systemów IT mogą starać się uzasadnić brak dostępu do dokumentacji względami bezpieczeństwa (tzw. "*security by obscurity*"), jednak podejście takie powinno być traktowane jako metoda ukrywania podatności i wad produktu.

- **Realizacja zasady "czterech oczu".** Co do zasady, certyfikacja oddziela role budowy systemu od jego oceny. Co więcej, strona certyfikująca powinna być **niezależna** od strony budującej system. Dzięki temu mniej prawdopodobne jest przymykanie oczu na określone wady systemu, na przykład pod presją konieczności uruchomienia go w krótkim terminie.

- **Wtórne wykorzystanie metod weryfikacji systemu.** Sprawdzenie własnego systemu poprzez opracowanie metodologii samodzielnie od podstaw jest trudne - wymaga zaangażowania odpowiednio doświadczonego personelu, zabiera stosunkowo dużo czasu i jest obarczone poważnym ryzykiem pominięcia szeregu istotnych kwestii. O wiele łatwiejsze jest użycie gotowych wymagań certyfikacyjnych i skoncentrowanie wysiłku na ewentualnym uzupełnieniu wymagań i procedur pod kątem specyficznych cech i funkcji badanego systemu.

- **Wyeliminowanie wpływu lokalnych ograniczeń i partykularnych interesów**. W przypadku budowania systemów i ich oceny na podstawie lokalnych, "narodowych" metod, istnieje zawsze niebezpieczeństwo oparcia się wyłącznie na lokalnych kompetencjach. W przypadku krajów średniej wielkości takich jak Polska, o relatywnie niewielkiej skali nakładów na badania i rozwój w zakresie informatyki, problem ten jest bardzo poważny. Co więcej, istnieje niebezpieczeństwo budowania wymagań pod konkretnych lokalnych interesariuszy - oferujących systemy bądź usługi badania jakości. W przypadku oparcia się o metody wypracowane w wyniku międzynarodowego konsensusu niebezpieczeństwo tego typu błędów i patologii jest dużo mniejsze (jakkolwiek trzeba również brać pod uwagę wpływ podmiotów dominujących).

- **Jednorazowy wysiłek w przypadku instytucji o zasięgu międzynarodowym**. Jedną z zasadniczych zalet schematów certyfikacji budowanych w oparciu o międzynarodowe gremia jest możliwość wykonania pojedynczego badania, które następnie ma znaczenie globalne. Nawet w przypadku schematów certyfikacji nie mających międzynarodowego formalnego statusu, praktyka rynku informatycznego wskazuje na olbrzymią rolę standardów, schematów i metod badań, bynajmniej nie opartych o instytucje publiczne bądź rolę przyznaną w systemie prawnym.

W zakresie efektywności ekonomicznej wskazać można na następujące czynniki, na które wpływ ma proces certyfikacyjny:

- **Relatywnie szybki wynik badania systemu.** O ile system budowany jest ze świadomością przyszłego procesu certyfikacji, badanie certyfikacyjne może być przeprowadzone sprawnie w stosunkowo krótkim czasie. Tym samym okres *"time to market"* może być znacząco zredukowany.

- **Zmniejszenie ryzyka działalności.** Prawidłowo przeprowadzony proces certyfikacyjny wpływa nie tylko na bezpieczeństwo o charakterze technicznym. Równie istotne jest **wykazanie należytej staranności** wobec klientów, partnerów gospodarczych, oraz organów nadzorujących. Ponieważ jedną z podstawowych wartości instytucji finansowej jest poziom wiarygodności, wpływa to na jej obiektywną wartość ekonomiczną.

- **Zmniejszenie skali ryzyka osobistego.** Pod względem technicznym nigdy nie będzie można mówić o absolutnym bezpieczeństwie produktów informatycznych[1]. Przy największym nawet stopniu ostrożności istnieje niezerowe prawdopodobieństwo wystąpienia krytycznych luk bezpieczeństwa. W przypadku ich wykrycia i wykorzystania przez środowiska przestępcze przed zastosowaniem odpowiednich zabezpieczeń, organy nadzoru i organy ścigania mogą ulec pokusie przerzucenia odpowiedzialności o charakterze karnym na osoby odpowiedzialne za systemy informatyczne w zaatakowanej instytucji finansowej.[2] **Przeprowadzenie certyfikacji w oparciu o powszechnie akceptowane i stosowane schematy certyfikacji pozwala wykazać zachowanie należytej staranności** i tym samym wykazać, że nie ma podstaw do postawienia zarzutów natury karnej.

Należy zaznaczyć, że pozytywne efekty certyfikacji niekoniecznie muszą wymagać współudziału instytucji mających formalny status, na przykład w postaci akredytacji przez podmioty publiczne. Wysoki poziom merytoryczny może być również osiągnięty w ramach współpracy organizacji finansowych i powołania do tego celu specjalnej niezależnej jednostki lub jednostek zajmujących się tymi zadaniami. Filozofia budowania w ten sposób systemów bezpieczeństwa jest stosowana w Wielkiej Brytanii i była w istocie zaczątkiem metodologii Common Criteria.

2.2. Certyfikacja a deklaracje producenta/operatora

Alternatywą dla metodologii opartej na certyfikacji przez niezależne jednostki jest podejście oparte na deklaracjach bezpieczeństwa producenta/operatora systemu. Niestety:

- deklaracje takie w najlepszym wypadku oparte są o powszechnie uznawaną listę wymagań, co w przypadku systemów tak specyficznych jak bankowość i infrastruktura rynków finansowych, może okazać się niewystarczające,

- nie należy oczekiwać, że podmiot prowadzący działalność z naruszeniem zasad sztuki akurat w momencie wydawania deklaracji wykaże się solidnością i przedłoży deklarację o własnej nierzetelności.

Doświadczenie uczy, że przy braku wymagań dotyczących istotnych treści deklaracji, informacje przedstawiane klientom mogą mieć charakter niemerytoryczny i ograniczać się do haseł o charakterze marketingowym.

Naczelną zasadą budowy systemów zaufania w systemach informatycznych musi być stosowanie zasady "nikt nie jest sędzią w swojej własnej sprawie". Deklaracje producenta/operatora mają głównie wartość w kontekście odpowiedzialności karnej oraz procesów cywilnych. Te ostatnie mogą mieć ograniczone znaczenie, bowiem szkody instytucji finansowej mogą znacznie przekraczać aktywa i wartość pozwanego nierzetelnego wykonawcy.

2.3. Certyfikacja a wymagania ochrony danych osobowych

Regulacja RODO[3] nakłada na podmioty przetwarzające dane osobowe nie tylko określone obowiązki w zakresie samego przetwarzania. Podmiot przetwarzający dane **musi być w stanie udokumentować, że wymagania stawiane przez RODO są spełnione** (*accountability*). Oznacza to, że:

- ciężar dowodu leży po stronie przetwarzającej dane,

- dowody powinny być przygotowane zawczasu do ewentualnej kontroli, a nie tworzone dopiero po przedstawieniu żądania.

[1] Zjawisko to ma głębokie przyczyny o charakterze matematycznym – tzw. nierozstrzygalność szeregu problemów o podstawowym znaczeniu dla ustalenia własności działania algorytmów.
[2] Tego typu efekt mrożący działa w przypadku instytucji publicznych ze względu na możliwość zastosowania art. 231 KK.
[3] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

Już sam brak dowodów na spełnienie wymagań RODO może być traktowany jako naruszenie zasad i może być związany z nałożeniem kar administracyjnych. Ich wysokość (zależność od obrotu rocznego w skali globalnej) może być szczególnie dotkliwa dla banków działających w skali międzynarodowej.

Regulacja RODO wprost zachęca do stosowania procedur certyfikacji (art. 42). Są to tylko zalecenia, jako że obowiązek był nierealizowalny w momencie wydania regulacji. Z drugiej strony, poddanie się procedurze certyfikacji stanowi niezwykle silny argument przeciwko zarzutom o ewentualne zaniedbania. W przypadku posiadania pozytywnego wyniku certyfikacji ewentualne zarzuty rozkładają się na bank, na podmiot certyfikujący, ale również na organy nadzorujące (UODO i organy europejskie).

Rozporządzenie RODO wprowadza również (art. 40) dodatkowy instrument: zatwierdzony kodeks postępowania (ang. *approved code of conduct*). W istocie mechanizm ten oparty jest na podobnej idei co certyfikacja. Podstawą jest opracowanie zasad działania (*code of conduct*) mających gwarantować prawidłową implementację zasad RODO. Zasady takie mogą być opracowane w szczególności przez sektor finansowy i przedłożone do akceptacji przez UODO. Istnieje również możliwość skorzystania z *codes of conduct* zaaprobowanych do stosowania w całej Europie przez organy europejskie. W ostatniej sytuacji bezpieczeństwo prawne podmiotu stosującego takie zasady jest bardzo wysokie.

2.4. Ograniczenia procedur certyfikacyjnych

Nie podlega wątpliwości, że certyfikacja niesie za sobą dużą wartość dodaną. Trzeba jednak mieć świadomość, że na procedury certyfikacyjne narzucone są pewne ograniczenia. Czasem rola certyfikacji bywa wyolbrzymiana, a w krańcowych przypadkach - może prowadzić do obniżenia poziomu cyberbezpieczeństwa poprzez złudne przekonanie co do wartości udzielonych gwarancji. Należy zdawać sobie sprawę, że:

- Certyfikacja sprawdza jedynie **zgodność** systemu z określonymi formalnymi cechami.
- Certyfikowane cechy muszą być łatwo weryfikowalne, zatem nie zawsze są to docelowe własności, jakie chciałaby osiągnąć jednostka poddająca swój system ocenie certyfikacyjnej.
- Proces certyfikacji różni się krańcowo od badania podatności systemów poprzez testowe próby ataku przeprowadzane na zlecenie organizacji poddającej się badaniu. Proces certyfikacji **skupiony jest na projekcie systemu i deklarowanych własnościach,** a nie na testowaniu systemu w warunkach rzeczywistych.
- Krytycznym zagadnieniem dla jakości wyniku certyfikacji nie jest sam proces badania systemu w ramach działań certyfikacyjnych, np. na podstawie dokumentów w rodzaju Protection Profile, wprowadzonych przez Common Criteria. Zadanie to jest stosunkowo rutynowe i nie wymaga aż tak wysokich kwalifikacji, jak etap wcześniejszy. **Zagadnieniem krytycznym jest sformułowanie i skonkretyzowanie odpowiednich wymagań bezpieczeństwa** - weryfikowalnych cech, które badany system powinien posiadać. Błędna lub niekompletna lista wymagań prowadzi w konsekwencji do wydania certyfikatu bezwartościowego pod względem celów, jakie chce osiągnąć jednostka poddająca się procesowi certyfikacji. Doświadczenie wskazuje na częste występowanie tego zjawiska - a niekiedy konsekwencje są bardzo głębokie[4].
- Proces certyfikacji z natury rzeczy **dotyczy kwestii raczej rutynowych**. Z tego też względu skuteczność certyfikacji jako metody zapobiegania subtelnym lukom bezpieczeństwa jest dość ograniczona.
- Narzucenie wymogu certyfikacji bezpieczeństwa przepisami prawa niesie za sobą pewne dodatkowe zagrożenia. Instytucje działające pod presją czasu i zmuszone do poddania swoich systemów lub produktów procesowi certyfikacji mogą skupiać swoją uwagę na wypełnianiu litery prawa, a nie na określeniu istotnych wymagań bezpieczeństwa. Na skutek tego sam **proces certyfikacji może dotyczyć kwestii mało istotnych** z punktu widzenia realnego cyberbezpieczeństwa. Co gorsza, certyfikacja narzucona przez regulacje prawne może **ograniczać wybór rozwiązań technologicznych** i prowadzić do konieczności wyboru rozwiązań nieoptymalnych pod względem bezpieczeństwa.

Mając na uwadze wszystkie ograniczenia i wady wymienione powyżej, należy jednak jeszcze raz podkreślić, że procesy o charakterze certyfikacyjnym **mogą być niezwykle istotnym i niezastąpionym środkiem prowadzącym do poprawy cyberbezpieczeństwa.**

[4] Dobrym przykładem tego typu jest przypadek estońskiego dowodu osobistego, który posiadał krytyczne słabości umożliwiające kryptoanalizę klucza publicznego skutkujące wyliczeniem klucza prywatnego zapisanego w dowodzie. Fakt ten nie podważył w jakikolwiek sposób wartości certyfikatów BSI udzielonych na mikrokontroler zawarty w estońskim dowodzie osobistym.

Dostępność gotowych rozwiązań dla zastosowania w sektorze bankowym

Raport dr Elżbiety Andrukiewicz[5] pośrednio pokazuje słabość dotychczasowej infrastruktury certyfikacyjnej w obszarze szczególnych potrzeb sektora instytucji finansowych. Sytuacja ta ma miejsce, mimo iż działania certyfikacyjne w sektorze obrotu finansowego nie są nowością.
Do najważniejszych **problemów** sektora bankowego, **związanych z potrzebą certyfikacji**, wyłaniających się w świetle tego opracowania należy zaliczyć:

- **Spory stopień koncentracji na zagadnieniach dotyczących terminali płatniczych.** Bardzo rozwinięty jest system certyfikacji związany z zagadnieniami obrotu bezgotówkowego przy użyciu terminali płatniczych. Jest to konsekwencja przyjętej architektury wymiany danych, w której bezpieczeństwo operacji jest uzależnione właśnie od bezpieczeństwa terminala.

  Niestety, znaczenie tych schematów certyfikacji jest skoncentrowane na rynku kart płatniczych i dotyczy głównie bezpieczeństwa z punktu widzenia organizacji świadczących usługi rozliczeniowe. Patrząc na kierunki rozwoju technologii stosowanych w obrocie finansowym, karty płatnicze zaczynają ustępować innym rozwiązaniom oferowanym przez *fintechy*.

  Najbardziej palące jest w obecnej chwili zagadnienie certyfikacji systemów komunikacji z klientem opartych na urządzeniach mobilnych. Obecnie stosowana praktyka postępowania to skanowanie kodu aplikacji w poszukiwaniu wrogiego kodu *(przez sklep z aplikacjami bądź na samym telefonie)*. Należy podkreślić jednak, że choć niewątpliwie są to działania znacząco zmniejszające skalę zagrożeń, nie dają one bezwzględnych gwarancji bezpieczeństwa – diagnostyka opiera się na wykrywaniu podejrzanych fragmentów kodu aplikacji.

Warto nadmienić, że bezpieczeństwo aplikacji webowych jest przedmiotem intensywnych prac. Warte odnotowania są choćby prace fundacji OWASP (Open Web Application Security Project) obejmujące tematykę bezpieczeństwa aplikacji webowych/mobilnych i metod ich testowania.

- **Brak utrwalonych praktyk certyfikacyjnych w zakresie ochrony danych osobowych**. Duża część danych przetwarzanych przez instytucje finansowe wpada do kategorii danych osobowych. Z drugiej strony, nawet gdy dane dotyczą stricte osób prawnych, to należałoby zastosować wobec nich te same albo prawie takie same mechanizmy ochrony w systemach informatycznych banków. Należy zwrócić uwagę na najnowsze idee legislacyjne: w Chińskiej Republice Ludowej wprowadzona została ustawa o cyberbezpieczeństwie, gdzie zakres ochrony nie został ograniczony do osób fizycznych.

Certyfikacja pod kątem ochrony danych osobowych jednocześnie mogłaby pokryć dużą liczbę zagadnień związanych z cyberbezpieczeństwem - tak naprawdę zasadniczym wyzwaniem dla wdrożenia RODO są zagadnienia o charakterze technicznym. Obowiązki w zakresie organizacyjnym, mimo że niekiedy uciążliwe, nie stawiają podmiotu przetwarzającego dane przed problemami, na które nie ma dziś odpowiedzi. Sytuacja w zakresie materii technicznej jest krańcowo inna - mimo dużego postępu w wielu obszarach, brak jest dojrzałych i niezawodnych rozwiązań dla wszystkich problemów. Z tego też powodu RODO odnosi się do aktualnego stanu techniki i wiedzy. Jednakże rozporządzenie RODO nie zwalnia podmiotów przetwarzających dane osobowe z obowiązku śledzenia jaki jest aktualny stan techniki i wiedzy i dostosowywania swoich systemów do tego stanu.

Ekspertyza dr Elżbiety Andrukiewicz nie wskazuje, aby prace nad powstaniem infrastruktury certyfikacyjnej pod kątem ochrony danych osobowych były w jakimś stopniu zaawansowane. W tej sytuacji pozostaje jedynie śledzić rozwój sytuacji pod kątem pojawienia się *code of conduct* opracowanego pod kątem sektora bankowego.

3.1. Początkowy poziom prac nad europejskim systemem certyfikacyjnym

Dane przytoczone w raporcie dr Elżbiety Andrukiewicz na temat europejskich ram systemów certyfikacji są dla sektora finansowego zarówno pozytywne, jak i niepokojące.

Jako aspekty o wydźwięku pozytywnym należy wymienić:

- **decyzję o budowie jednolitego europejskiego systemu certyfikacji** – w przeciwnym razie grozi rozczłonkowanie rynku usług certyfikacyjnych na poziom narodowy z koniecznością wielokrotnego ponoszenia wydatków, problemy związane z niekompatybilnością certyfikatów i procedur certyfikacyjnych - zarówno pod względem prawnym jak i technicznym czy niski poziom merytoryczny w niektórych krajach (działać może zasada *wypierania z rynku dobrego pieniądza przez zły pieniądz*). Stopień skomplikowania technicznego i rozmiar

[5] dr inż. Elżbieta Andrukiewicz „Certyfikacja produktów i usług teleinformatycznych z uwzględnieniem potrzeb sektora bankowego"

zadań wskazuje, że ich kompleksowa realizacja jest możliwa tylko na płaszczyźnie europejskiej (biorąc pod uwagę np. zasoby dostępnych specjalistów).

- **krokowy program wdrażania koncepcji** - koncepcja taka jest pragmatyczna i realistyczna. Dysponując ograniczonymi zasobami ludzkimi i przede wszystkim brakami w zakresie *know how,* lepiej jest się skupić na kilku (krytycznych) obszarach i rozwiązać do końca najpilniejsze potrzeby, niż rozpocząć prace na wielu polach. Doświadczenia zdobyte na wycinkowych polach mogą później przyspieszyć proces certyfikacji w pozostałych obszarach.

Niestety należy wymienić również spostrzeżenia negatywne:

- **perspektywa czasowa** - może się okazać, że obszary certyfikacji specyficzne dla instytucji finansowych nie będą procedowane wystarczająco szybko w stosunku do pojawiających się potrzeb sektora finansowego. Z drugiej strony, mogą pojawiać się dążenia do objęcia usług finansowych w kluczowych obszarach obowiązkową certyfikacją, rozszerzając wymagania Dyrektywy NIS[6].

- **rola instytucji publicznych -** w projektowanym systemie certyfikacji kluczową rolę mają odgrywać instytucje publiczne. Taki kształt systemu zapewne doskonale się sprawdzi w przypadku krajów, w których od jakiegoś czasu funkcjonują już instytucje publiczne odpowiedzialne za zagadnienia cyberbezpieczeństwa na rynku wewnętrznym. Kluczowym jest zdobyte doświadczenie, potencjał merytoryczny tych instytucji oraz możliwości pozyskania i utrzymania zasobów kadrowych o unikalnych kwalifikacjach. W Polsce stworzenie odpowiednich instytucji może napotkać na barierę kadrową: specjaliści w tym obszarze są trudni do znalezienia, zaś wynagrodzenia oferowane przez sektor IT mogą wielokrotnie przekraczać ofertę podmiotów publicznych.

3.2. Stan procedur certyfikacyjnych dla rozwiązań chmurowych

Przytoczone w raporcie dr Elżbiety Andrukiewicz informacje wskazują, że certyfikacja rozwiązań chmurowych nadal może być wyzwaniem. Nie jest to zbytnim zaskoczeniem, biorąc pod uwagę stan technologii: dla przykładu nie wiadomo, jak skutecznie przeciwdziałać tzw. *cache attacks* umożliwiających wydobycie klucza szyfrującego używanego przez proces innego użytkownika (atak odbywa się bez naruszenia zasad wirtualizacji i bez zdobycia dodatkowych uprawnień).

Niewątpliwie obszarem przetwarzania danych w chmurze może być analiza danych w celach strategicznych (np. dla rozpoznania istotnych zjawisk o charakterze makroekonomicznym). Należy tu zwrócić uwagę na gorące dyskusje toczące się na ten temat - konieczność znalezienia kompromisu pomiędzy analizą danych i cyberbezpieczeństwem.[7] Należy również zwrócić uwagę, że większość problemów nie dotyczy chmury prywatnej. Problemy dotyczą jednak małych podmiotów, dla których rozwiązania chmurowe mogłyby stanowić szansę pokonania szeregu problemów wynikających z małej skali działania.

[6] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.

[7] Zagadnienia te są przedmiotem silnych sporów w Chinach wobec ograniczeń narzucanych przez ustawę o cyberbezpieczeństwie. Firmy zajmujące się analizą danych wskazują, że rygorystyczne przestrzeganie zasad ochrony może doprowadzić do zmniejszenia konkurencyjności chińskiej gospodarki na rynku globalnym.

ROZDZIAŁ IV
Zalecenia dotyczące strategii implementacji

Omawiany raport dr Elżbiety Andrukiewicz wskazuje na konieczność budowy systemów informatycznych banków z uwzględnieniem powstających systemów certyfikacji europejskiej, biorąc pod uwagę prawdopodobieństwo przyszłego obowiązku takiej certyfikacji. Jest to z pewnością słuszne zalecenie, jednak jego realizacja może być trudna ze względu na brak szczegółowych informacji na temat przyszłych schematów certyfikacji. Ruchem wyprzedzającym może być przejęcie inicjatywy na polu systemów instytucji bankowych. Byłoby to podejście tym bardziej pragmatyczne, że zasadnicze zadania merytoryczne będą wykonywane przez powołane ad hoc zespoły specjalistów. Sektor finansowy powinien być przygotowany do delegowania dobrze przygotowanych specjalistów ze swojej strony.

Zalecenie 1

Zadania w zakresie przygotowania do certyfikacji systemów bankowych powinny być prowadzone wspólnie dla całego sektora finansowego przez zespoły powołane i finansowane przez środowisko bankowe. Pozwoliłoby to na:

- przygotowanie procesów odpowiadających specyficznym potrzebom i wymaganiom wobec systemów informatycznych sektora finansowego,
- odpowiednią reprezentację całego sektora bankowego, w tym zarówno podmiotów dominujących, jak i małych jednostek spółdzielczych,
- uniknięcie niebezpieczeństwa narzucenia nieuzasadnionych merytorycznie wymagań, zgłaszanych przez instytucje oferujące usługi certyfikacyjne w celu maksymalizacji zysku.

W miarę możliwości należałoby zadania te realizować w porozumieniu/współpracy z innymi krajami Europy.

Zalecenie 2

Zasadniczym zadaniem jest nie samo przeprowadzenie certyfikacji, ale sformułowanie wymagań i wybór metodologii certyfikacyjnej. Samo prowadzenie certyfikacji powinno być działaniem relatywnie rutynowym.

Instytucje finansowe powinny co najmniej uczestniczyć w tym procesie. Wskazane byłoby wręcz wiodące działanie w tym zakresie, przy zastrzeżeniu mocnego zaangażowania innych stron, w tym na przykład przedstawicieli producentów instrumentów cyberbezpieczeństwa czy instytucji badawczych. Udział przemysłu powinien zapobiec sformułowaniu odwołań do rozwiązań będących wciąż w sferze *science fiction.*

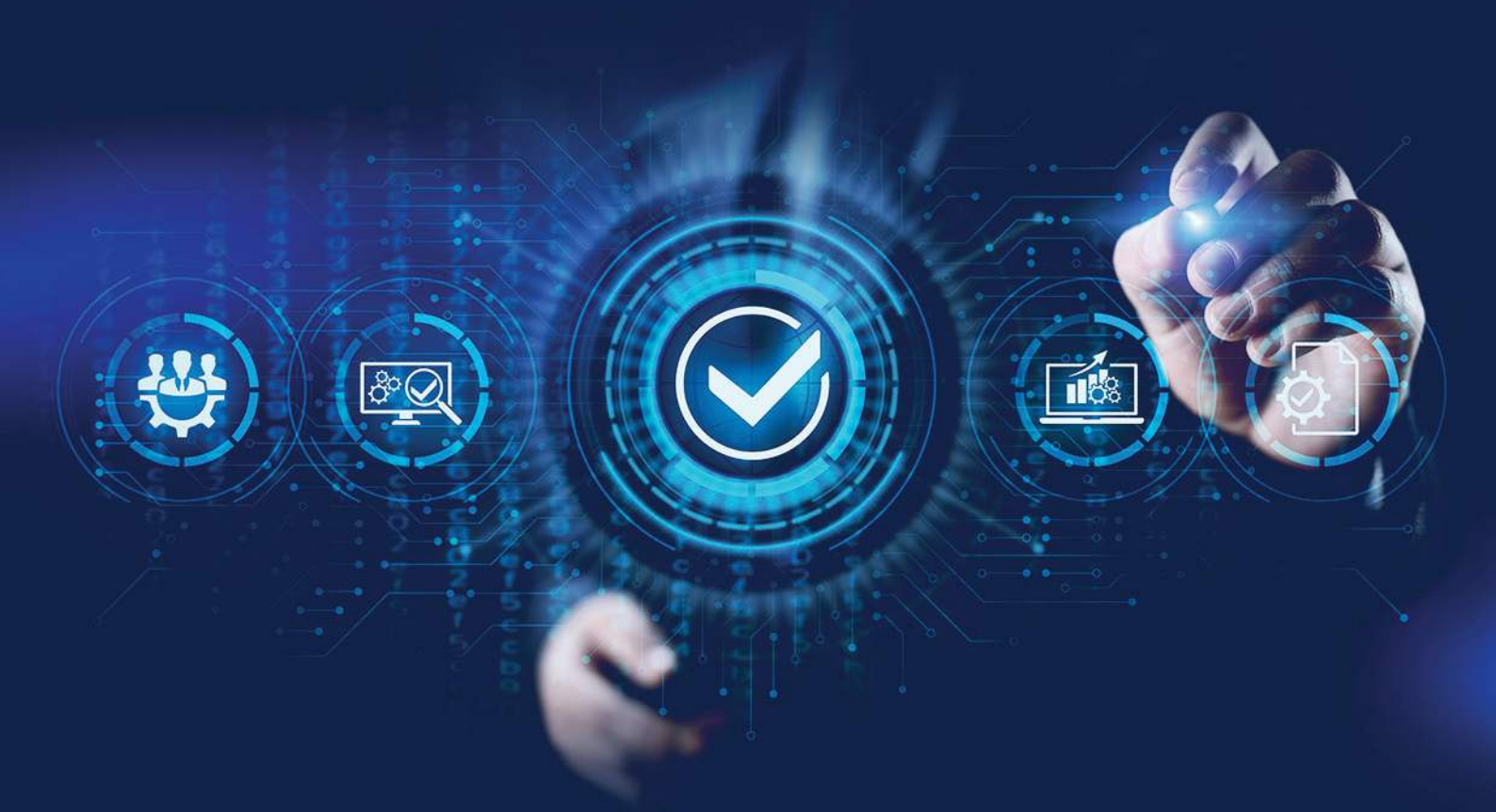
Zalecenie 3

Sektor finansowy mógłby skorzystać z możliwości danych przez Rozporządzenie RODO i opracować *codes of conduct* dla ochrony danych osobowych w instytucjach finansowych. Zatwierdzenie takich reguł i ich wdrożenie (być może wsparte wewnętrznym systemem certyfikacji sektora finansowego) mogłoby być ruchem wyprzedzającym, przy okazji regulującym wiele kluczowych zagadnień cyberbezpieczeństwa.

Niestety nie jest to zadanie łatwe. Zasadniczo słuszne zasady wprowadzone przez RODO wymagają rozwiązania nietrywialnych kwestii szczegółowych - zarówno w obszarze prawnym, jak i technicznym, a jak pośrednio wskazuje omawiany raport dr Andrukiewicz - trudno jest liczyć na silne wsparcie zewnętrzne organów regulacyjnych[8].

[8] Przejawem tego typu zjawisk jest raport ENISA na temat elektronicznej identyfikacji, gdzie zamiast twardych, konkretnych rekomendacji technicznych przedstawione jest zalecenie, by podmioty gospodarcze wykazywały ostrożność i śledziły rozwój technologii.

Szczególne wyzwania związane z ochroną danych osobowych[1]



[1] Niniejszy fragment raportu wykorzystuje rezultaty dyskusji naukowej prowadzonej z prof. Moti Yungiem z Columbia University.

Jak wskazujemy powyżej, jedną z pragmatycznych strategii działania jest związanie certyfikacji z realizacją wymagań rozporządzenia RODO. Wydawać by się mogło, że taka droga jest pozbawiona niepewności i wyzwań o charakterze merytorycznym. Nie do końca tak jest – na styku regulacji prawnych i realiów systemów powstaje wiele pytań, na które brak jest odpowiedzi ugruntowanych powszechnie w doktrynie prawnej. Poniżej sygnalizujemy kilka takich problemów.
Niniejszy rozdział ma na celu ostrzeżenie, że odpowiedzi na stawiane pytania mogą mieć olbrzymi wpływ na dopuszczalne sposoby przetwarzania danych osobowych.

Dopuszczalność agregacji danych. O ile przetwarzanie danych klienta instytucji finansowej w celu realizacji usług prowadzonych bezpośrednio dla klienta nie może budzić żadnych zastrzeżeń formalnych, to przetwarzanie w celach, które nie służą obsłudze klienta, ochronie jego interesów czy ochronie systemów informatycznych banku lub istniejących zobowiązań prawnych – już takie wątpliwości budzą. Rozporządzenie RODO traktowane literalnie nie pozwala na użycie danych w żadnym celu wykraczającym poza przypadki wymienione w art. 6.

Dopuszczalność anonimizacji danych. Wiele problemów mogłoby być rozwiązanych poprzez wykorzystanie np. do celów analitycznych danych zanonimizowanych. Dane takie nie podlegają ochronie RODO, jako że dane takie nie dotyczą możliwej do zidentyfikowania osoby. Jednak proces anonimizacji wymaga użycia danych osobowych, a tych można użyć tylko w sposób przewidziany w umowie lub obowiązującym prawie.

Niebezpieczeństwa związane z przetwarzaniem danych "nieosobowych". Brak kwalifikacji jako dane osobowe nie oznacza bezwarunkowo trafności takiej kwalifikacji. Może się okazać, że w konfrontacji z innymi danymi dostępnymi publicznie (o których przetwarzający podmiot może nie wiedzieć), dane te mają atrybut danych osobowych. Rozporządzenie RODO nie specyfikuje, jakie jest praktyczne znaczenie "możliwej do zidentyfikowania osoby". Należy mieć świadomość, że nawet przy korzystnej, pragmatycznej interpretacji, ewentualne wątpliwości mogą być źródłem skarg i sporów zarówno cywilnych, jak i z UODO.

Komplikacje związane z danymi osobowymi więcej niż jednej osoby. Rozporządzenie zakłada milcząco, że dane osobowe dotyczą pojedynczej osoby fizycznej. Istnieją przypadki, gdy danych takich nie daje się rozdzielić na dane poszczególnych "współwłaścicieli". W takim przypadku nie wiadomo na przykład, jak realizować prawo do "bycia zapomnianym".

Kategoryzacja danych jako osobowe i nieosobowe. Określenie atrybutu danych jak "osobowe" lub "nieosobowe" (o ile zachodzi taka potrzeba) powinno być w znacznym stopniu zautomatyzowane. O ile w wielu przypadkach jest oczywiste, że mamy do czynienia z danymi osobowymi, to przypadkiem trudnym jest określenie, co już nie jest danymi osobowymi. Na przykład określenie, czy wynik zapytania do bazy danych stanowi dane osobowe - może być dalece nietrywialne. Istnieją na ten temat interesujące koncepcje teorio-informacyjne (np. *differential privacy*), jednak rozwiązania te są skomplikowane i mało realne do zastosowania w praktyce.

Wnioski końcowe

Wprowadzenie procedur certyfikacji systemów bankowych wydaje się zarówno niezbędne (jako środek ostrożnościowy w celu eliminacji szeregu zagrożeń technicznych), jak i nieuniknione (ze względu na powstający europejski system cyberbezpieczeństwa czy wymagania regulacji europejskich).

W dłuższej perspektywie czasowej można liczyć na powstanie europejskiego systemu certyfikacji. Jednak bez inicjatywy i aktywnego udziału sektora bankowego, system certyfikacji systemów bankowych może być budowany niewystarczająco szybko w stosunku do potrzeb. Oddolne budowanie zrębów tego systemu przez sektor bankowy mogłoby znacząco przyspieszyć ten proces.

Wykorzystanie potencjału tkwiącego w certyfikacji zależy przede wszystkim od dobrego przeprowadzenia tego procesu. Krytycznym etapem jest faza pierwsza – sformułowanie wymagań, reguł certyfikacji itp. Faza ta wymaga głębokiego zaangażowania szerokiej grupy specjalistów.

Program certyfikacji powinien być realizowany w miarę możliwości wspólnie przez cały sektor na podstawie wspólnych kryteriów i wspólnej metodologii.