BEZPIECZEŃSTWO TELEINFORMATYCZNE TRANSAKCJI FISKALNYCH

RAPORT

FUNDACJA bezpieczna cyberprzestrzeń

RAPORT
BEZPIECZEŃSTWO TELEINFORMATYCZNE TRANSAKCJI FISKALNYCH

Spis treści

1 Geneza raportu

Przedstawiciele administracji publicznej w 2016 r. przedstawili szereg pomysłów na rozwój technologiczny systemów odpowiedzialnych za szeroko rozumiane transakcje fiskalne. Jednym z nich jest koncepcja „e-paragon", która zakłada stopniową rezygnację z paragonów w formie papierowej i bezpośredni dostęp administracji do danych ze wszystkich transakcji „online".

W wypowiedziach prasowych decydentów oraz branżowych ekspertów bardzo rzadko pojawiał się jednak aspekt bezpieczeństwa teleinformatycznego proponowanych rozwiązań, który ze względu na znaczenie przetwarzanych danych, np.: zawierających dane osobowe, powinien być jednym z najistotniejszych czynników decydujących o kierunku rozwoju i wyborze metod realizacji technicznych.

W dyskusjach rola bezpieczeństwa teleinformatycznego, ochrony prywatności klientów i przedsiębiorców była marginalna.

Biorąc pod uwagę powyższe trendy, Fundacja Bezpieczna Cyberprzestrzeń, której jednym z zadań statutowych jest uświadamianie o zagrożeniach w sferze cyberprzestrzeni, postanowiła w niniejszym raporcie przedstawić najważniejsze informacje o ochronie teleinformatycznej i ochronie prywatności oraz skonfrontować je z koncepcjami będącymi przedmiotem dyskusji publicznej.

2 Wstęp

W połowie 2016 r. w mediach pojawiła się seria artykułów[1] prasowych poświęconych tzw. koncepcji „e-paragon" przygotowanej przez Ministerstwo Rozwoju. Zgodnie z informacjami medialnymi, jej celem ma być rezygnacja z przetwarzania paragonów w postaci papierowej (paragon fiskalny - wydrukowany przez kasę dla nabywcy w momencie sprzedaży dokument potwierdzający dokonaną transakcję sprzedaży).

Uzasadnień dla takiej koncepcji (paragonów w formie elektronicznej) administracja publiczna przedstawia wiele, wymieniając korzyści dla poszczególnych interesariuszy. Klientom jak i handlowcom propozycja ma pomóc w procesie przechowywania tych dokumentów. Państwu ma zapewnić wzrost z wpływów z podatku VAT, jak się szacuje, o 2 do 3 mld zł rocznie. Ma być również zwiększona skala obrotu bezgotówkowego. Administracja zakłada bowiem, że decydując się na takie rozwiązanie, ograniczone zostaną praktyki polegające na nielegalnym obrocie towarami i usługami – ograniczona zostanie „szara strefa".

Aby tego dokonać, konieczne jest wdrożenie nowych rozwiązań technicznych, które strona rządowa w koncepcji „e-paragon" proponuje – szczególnie w kontekście wymagań dla kas rejestrujących (kasy rejestrujące obrót i wyliczające kwoty należnego podatku). Dodatkowo jednym z głównych założeń nowych rozwiązań jest budowa centralnego repozytorium paragonów zarządzanego przez osobną spółkę - Aplikacje Krytyczne. Repozytorium to stanowiłoby centralny rejestr paragonów, który byłbym podstawowym zasobem danych analitycznych dla kontroli skarbowej.

Kolejnym z nowatorskich pomysłów jest integracja kas fiskalnych z terminalami płatniczymi, co spowodowało by udostępnienie cennych danych agentom rozliczeniowym i bankom. Do tego wymagana jest zmiana aktów wykonawczych i działań jednostki dokonującej homologacji urządzeń – Głównego Urzędu Miar.

Dlatego Ministerstwo Rozwoju nowelizuje rozporządzenie w sprawie kryteriów i warunków technicznych, którym muszą odpowiadać kasy rejestrujące obrót w sklepach i punktach usługowych. Nowe kasy mają rejestrować sprzedaż tylko elektronicznie, a docelowo handlowcy mieliby zaprzestać wydawania papierowych paragonów i zastąpić je elektronicznymi.

Dodatkowo, za zgodą klienta, dane mogłyby trafiać bezpośrednio do systemów bankowych, co zdaniem Ministerstwa Rozwoju, przyniesie same korzyści - paragon będzie na trwałym nośniku, dzięki czemu łatwiej będzie reklamować produkty, a z drugiej strony banki i przedsiębiorstwa będą mogły oferować swoim klientom dodatkowe usługi: zarządzania budżetem, programy lojalnościowe etc.

[1] m.in. http://biznes.gazetaprawna.pl/artykuly/955606,e-paragon-tylko-w-sieci.html

Celem administracji jest również promocja obrotu bezgotówkowego. Docelowo klienci, którzy nie będą chcieli korzystać z kart płatniczych i zapłacą za towary i usługi gotówką, paragon otrzymywać będą po podaniu numeru karty programu lojalnościowego, adresu e-mail lub numer telefonu, a sprzedawca (a właściwie jego kasa) prześle mu elektroniczny paragon.

Przedstawiciele handlowców zwracają jednak uwagę na wysoki koszt wymiany urządzeń, który szczególnie dotkliwy będzie dla małych przedsiębiorstw. Również małe przedsiębiorstwa, położone na terenach wiejskich, mają najwięcej wątpliwości co do wymagań technicznych, np. stałego dostępu do sieci Internet i bieżącego przesyłania danych, co może się okazać szczególnie istotne, gdyż w przypadku braku skutecznej komunikacji może dojść do blokady kasy. Wciąż jeszcze wysoki (większościowy) jest odsetek transakcji gotówkowych, które w przypadku systemu e-paragon, wychodzą poza ramy obecnego projektu.

Zastrzeżenie artykułowane są również przez inne resorty obawiające się zbyt dużej roli podmiotów trzecich w procesie rozliczeń transakcji, np. banków, które mogłyby dysponować bardzo dużym zasobem danych o zachowaniach klientów.

Niniejszy raport doda do opisanej powyżej dyskusji jeszcze jeden aspekt – bezpieczeństwa teleinformatycznego.

3 Fundacja Bezpieczna Cyberprzestrzeń

Fundacja Bezpieczna Cyberprzestrzeń (FBC) powstała w czerwcu 2010 roku. Celem Fundacji jest działanie na rzecz bezpieczeństwa cyberprzestrzeni, w tym na rzecz poprawy bezpieczeństwa w sieci Internet. Osiągnięcie tych celów fundacja realizuje poprzez działalność w trzech głównych obszarach:

- UŚWIADAMIANIA o zagrożeniach teleinformatycznych,
- REAGOWANIA na przypadki naruszania bezpieczeństwa w cyberprzestrzeni,
- prowadzenia DZIAŁALNOŚCI BADAWCZO-ROZWOJOWEJ w dziedzinie bezpieczeństwa teleinformatycznego.

FBC zaangażowana jest w wiele inicjatyw, konferencji, szkoleń i projektów dotyczących tematyki bezpieczeństwa teleinformatycznego. Tworzy i współtworzy raporty i opracowania z tematyki bezpieczeństwa teleinformatycznego i ochrony infrastruktury krytycznej, jak również wiele materiałów szkoleniowych z zakresu bezpieczeństwa IT wykorzystywanych w kraju i zagranicą.

Fundacja w 2012 roku zainicjowała, współorganizowała i koordynowała pierwsze w Polsce ćwiczenia z ochrony w cyberprzestrzeni – Cyber-EXE Polska 2012, które były kontynuowane w roku 2013, 2014, 2015 i również planowane są w latach następnych.

Ponadto Fundacja blisko współpracuje również z Europejską Agencją Bezpieczeństwa Sieci i Informacji (ENISA), Stowarzyszeniem CEENet (Central Eastern European Network Association). Fundacja jest członkiem APWG (The Anti-Phishing Working Group) oraz jest członkiem polskiego forum zespołów reagujących i zespołów bezpieczeństwa – ABUSE- FORUM.

Fundacja ma swój udział w tworzeniu periodyka „CIIP focus" wydawanego przez Rządowe Centrum Bezpieczeństwa, jest również wydawcą biuletynu „Zawór Bezpieczeństwa".

FBC jest wydawcą pierwszego polskiego podcastu dotyczącego tematu bezpieczeństwa teleinformatycznego „Cyber…Cyber…" .

W roku 2015 FBC zainaugurowała Stowarzyszenie – Polska Obywatelska Cyberobrona (POC), które dzięki wiedzy i doświadczeniom swoich członków tworzy potencjał do wykorzystania przez polskie struktury odpowiedzialne za bezpieczeństwo teleinformatyczne.

Fundacja Bezpieczna Cyberprzestrzeń organizuje jedną z największych konferencji w Polsce poświęconych bezpieczeństwu teleinformatycznemu – konferencję SECURITY CASE STUDY.

4 Cel i zakres raportu

Celem niniejszego raportu jest przedstawienie zagrożeń dla przewidywanych rozwiązań technologicznych ich potencjalnym użytkownikom, czyli klientom, przedsiębiorcom, producentom rozwiązań technologicznych oraz przedstawicielom administracji publicznej jak również sporządzenie rekomendacji w zakresie kierunków rozwoju projektów związanych z informatyzacją transakcji fiskalnych.

Zakresem raportu objęte zostaną najczęściej pojawiające się w dyskusjach koncepcje, które przedstawione zostaną w niniejszym raporcie jako trzy potencjalne fazy wdrożenia projektu „e-paragon":

1. Modyfikacja kas rejestrujących o funkcje automatycznego przesyłania danych do centralnego repozytorium oraz budowa tejże bazy danych;
2. Koncepcja zastąpienia dedykowanych kas rejestrujących przez oprogramowanie instalowane na dowolnej platformie sprzętowej;
3. Wyłączenie ze stosowania formy papierowej paragonu (zarówno kopii podatnika jak i klienta).

5 Kontekst

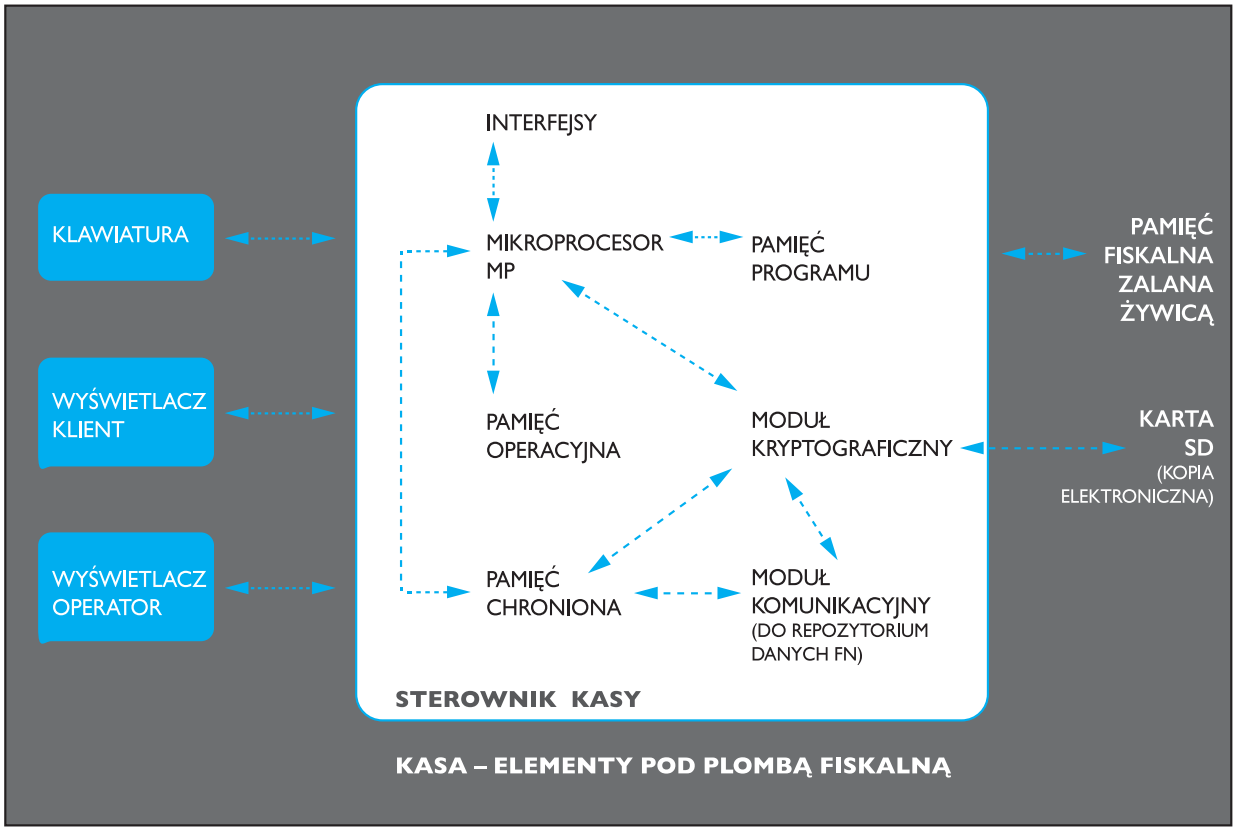
Dla zbudowania jak najbardziej pełnego obrazu sytuacji potencjalnego rozwoju projektu „e-paragon", w niniejszym raporcie przedstawione zostanie on w czterech kontekstach: technologicznym, prawnym, finansowym i społecznym.

5.1 Kontekst Technologiczny

Przedsiębiorcy rozpoczynający prowadzenie działalności gospodarczej muszą rozpocząć m.in. dokumentowanie zawieranych transakcji. Uzyskane ze sprzedaży przychody wprowadzane są następnie do odpowiednich ewidencji. Najbardziej rozpowszechnioną formą ewidencjonowania są kasy fiskalne.

Kasa fiskalna, inaczej rejestrująca, ma za zadanie rejestrowanie obrotu dotyczącego sprzedaży detalicznej.

Rysunek 1 Schemat budowy kas wg wymagań rozporządzenia Ministra Gospodarki z dnia 27.08.2013 r. w sprawie kryteriów i warunków technicznych, którym muszą odpowiadać kasy rejestrujące) (Dz. U. z 2013 r. Poz. 1076 ze zm.).



Rysunek 2 Schemat budowy kas wg projektu rozporządzenia Ministerstwa Rozwoju w sprawie kryteriów i warunków technicznych, którym muszą odpowiadać kasy rejestrujące z dnia 17.08.2016 r.

Przed uruchomieniem kasy należy dokonać fiskalizacji kasy, czyli jednokrotnego i niepowtarzalnego procesu inicjującego pracę pamięci fiskalnej kasy oraz pamięci chronionej kasy (wg nowych wymagań), zakończony wydrukiem raportu fiskalnego fiskalizacji, po którym niemożliwe jest uruchomienie kasy w trybie niefiskalnym.

Pamięć chroniona jest to urządzenie zawarte w kasie, zawierające elektroniczny nośnik danych, umożliwiające zapis i odczyt dokumentów fiskalnych i niefiskalnych emitowanych przez kasę pod bezpośrednią kontrolą programu pracy kasy, w sposób uniemożliwiający ich zmianę bez wykrycia tego zdarzenia w trakcie weryfikacji zapisów z zawartością pamięci fiskalnej.

Pamięć fiskalną z kolei rozumie się urządzenie zawarte w kasie, zawierające elektroniczny nośnik danych, umożliwiające niezmieniany zapis danych pod kontrolą programu pracy kasy.

Moduł kryptograficzny definiowany jest jako urządzenie zawarte w kasie, odpowiedzialne za generowanie podpisów cyfrowych dokumentów fiskalnych i niefiskalnych emitowanych przez kasę.

Należy zwrócić również uwagę na szereg wymagań przewidywanych nowymi przepisami w zakresie konstrukcji kas rejestrujących oraz wymagań dotyczących przechowywania danych w pamięciach kas rejestrujących.

Kasy będą musiały również współpracować z tzw. repozytorium (centralna baza danych z transakcji obsługiwana przez fiskusa) z wykorzystaniem protokołu komunikacyjnego. Do każdej kasy przypisana zostanie unikalna para kluczy asymetrycznych, z których klucz prywatny przechowywany będzie w kasie i wykorzystywany do podpisywania dokumentów fiskalnych i niefiskalnych, natomiast klucz publiczny w postaci certyfikatu wydanego przez repozytorium wykorzystywany będzie do weryfikacji tych dokumentów przez repozytorium. Transmisja danych z kas do repozytorium będzie zabezpieczona pod względem poufności i integralności zgodnie z protokołem TLS w wersji 1.0 lub wyższej, z wykorzystaniem certyfikatów elektronicznych w standardzie PN-ISO/IEC 9594-8:2006 x.509. lub wyższym. Podczas komunikacji kasy z repozytorium musi nastąpić uwierzytelnienie nadawcy i odbiorcy, przy czym podstawą

uwierzytelnienia w kasie muszą być mechanizmy oparte o tzw. silne uwierzytelnienie (infrastruktura klucza publicznego).

Wszystkie operacje kryptograficzne będą musiały zapewniać poufność, integralność i uwierzytelnienie danych i będą musiały być realizowane przez moduł kryptograficzny kasy, którego bezpieczeństwo musi być zapewnione zgodnie ze standardem NIST FIPS 140-2 level 2 lub wyższym lub ISO/IEC 11889-1:2015 TPM 2.0 lub wyższym.

Największa słabość nowych przepisów dotyczy wprowadzania kilku dodatkowych interfejsów np. zapewniających współpracę z terminalem płatniczym czy innymi urządzeniami i systemami, które w zautomatyzowany sposób przesyłały by paragony lub pełne dane zakupowe w formie elektronicznej. Generują one bowiem szereg podatności, a uzasadnienie ich stosowania nie jest jednoznaczne z punktu widzenia bezpieczeństwa teleinformatycznego lub odpowiednie ich specyfikacje nie są opublikowane.

5.2 Kontekst Prawny

Główne zagadnienia prawne dotyczące kas rejestrujących znajdują są w niżej wymienionych aktach prawnych:

- Ustawa z dnia 11.03.2004 r. o podatku od towarów i usług (Dz. U. z 2011 r. nr 177, poz. 1054 ze zm.) Dział XI Rozdział 3 Art. 111 Kasy rejestrujące;
- Rozporządzenie Ministra Finansów z dnia 4.11.2014 r. w sprawie zwolnień z obowiązku prowadzenia ewidencji przy zastosowaniu kas rejestrujących (Dz. U. z 2014 r. poz. 1544);
- Rozporządzenie Ministra Finansów z dnia 14.03.2013 r. w sprawie kas rejestrujących (Dz. U. z 2013 r. Poz. 363 ze zm.);
- Rozporządzenie Ministra Gospodarki z dnia 27.08.2013 r. w sprawie kryteriów i warunków technicznych, którym muszą odpowiadać kasy rejestrujące) (Dz. U. z 2013 r. Poz. 1076 ze zm.).
  Ostatni z wymienionych dokumentów będzie zmieniony w celu przystosowania kas do nowych wymagań koncepcji „e-paragon". W konsultacjach jest obecnie najważniejszy dla niniejszego raportu dokument:
    - Projekt rozporządzenia Ministerstwa Rozwoju w sprawie kryteriów i warunków technicznych, którym muszą odpowiadać kasy rejestrujące z dnia 17.08.2016 r.

Poniżej zaprezentowano ogólne założenia projektu oraz opinię prawną opublikowaną przez Fundację Panoptykon. Wg. oświadczenia pracowników Ministerstwa Rozwoju. w najbliższym czasie spodziewać należy się również rozporządzenia określającego wymagania wobec centralnego repozytorium paragonów. Będzie ono miało kluczowe znaczenie dla możliwości oceny aspektów bezpieczeństwa związanych z repozytorium.

5.2.1 Projekt rozporządzenia Ministerstwa Rozwoju w sprawie kryteriów i warunków technicznych, którym muszą odpowiadać kasy rejestrujące

Projekt rozporządzenia zawiera zbiór szczegółowych wymagań technicznych i może stanowić swoistą listę kontrolną dla Głównego Urzędu Miar przy homologacji urządzeń. Uzasadnienie przedstawia zakres i przyczyny zmian w stosunku do obecnie funkcjonującego rozporządzenia z roku 2013 r. i dlatego warto przytoczyć je w całości:

Na podstawie art. 111 ust. 8 ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług minister właściwy do spraw gospodarki, w porozumieniu z ministrem właściwym do spraw finansów publicznych określa, w drodze rozporządzenia:

1) szczegółowe kryteria i warunki techniczne, którym muszą odpowiadać kasy rejestrujące, oraz sposób oznaczania pamięci fiskalnej kas rejestrujących numerami unikatowymi, warunki ich przydzielania oraz dokumenty, które powinny być dołączone do kasy rejestrującej przy wprowadzaniu jej do obrotu,

2) dane, które powinien zawierać wniosek producenta krajowego albo podmiotu dokonującego wewnątrzwspólnotowego nabycia lub importu kas rejestrujących o wydanie potwierdzenia Prezesa Głównego Urzędu Miar, że:

- kasy te zapewniają prawidłowe zaewidencjonowanie podstawowych danych dotyczących zawieranych transakcji oraz zapewniają przechowywanie tych danych lub zapewniają bezpieczny ich przekaz na zewnętrzne nośniki danych

- spełniają kryteria i warunki techniczne, którym muszą odpowiadać, jak również rodzaje dokumentów, w tym oświadczeń, oraz kas rejestrujących wzorcowych do badań i innych urządzeń, które mają być przedstawione lub dostarczone wraz z wnioskiem,

3) okres, na który jest wydawane wspomniane potwierdzenie Prezesa Głównego Urzędu Miar,

4) zakres badań kas rejestrujących oraz rodzaje danych zawartych w sprawozdaniu z wyników badań wykonywanych Prezesa Głównego Urzędu Miar.

Głównym celem wydania nowego rozporządzenia, zastępującego rozporządzenie Ministra Gospodarki z dnia 27 sierpnia 2013 r. jest dostosowanie regulacji do możliwości emisji dokumentów fiskalnych i niefiskalnych w dwóch formach – elektronicznej i papierowej. Dotychczasowe przepisy umożliwiały jedynie wydruk takich dokumentów. Wobec postępu technologicznego oraz możliwości ich wykorzystania dla zwiększenia wpływów fiskalnych z transakcji ewidencjonowanych paragonami, przy jednoczesnym zapewnieniu możliwości współpracy kasy rejestrującej z terminalem płatniczym, dzięki określeniu zasad komunikacji obu typów urządzeń.

Rozporządzenie znosi też możliwość archiwizacji paragonów w postaci papierowej zastępując ją przechowywaniem w pamięci chronionej i pamięci fiskalnej.

Celem projektowanego aktu wykonawczego do ustawy o podatku od towarów i usług jest zwiększenie akceptacji płatności bezgotówkowych oraz zapewnienie konsumentom dostępu do paragonów elektronicznych w jednym miejscu. Celem jest również wprowadzenie nowego standardu protokołu komunikacyjnego dla nowych urządzeń fiskalnych wchodzących do eksploatacji. Jednocześnie celem jest możliwie szybkie wycofanie z eksploatacji urządzeń, które są przestarzałe i nie mogą być dostosowane do nowych wymagań.

Funkcjonujący obecnie system fiskalizacji jest bezpieczny, a system homologacji weryfikujący bezpieczeństwo urządzeń fiskalnych ustandaryzowany. Brak jednak centralnego systemu do analizy i kontroli transakcji sprzedaży, a systemy i urządzenia fiskalne są niedostosowane do realizacji centralnego raportowania transakcji. Aby było to możliwe potrzebny jest powszechny standard połączenia kas fiskalnych z centralnym repozytorium a także z terminalami płatniczymi. Dodatkowo, raportowanie i dokumenty oparte o wydruki, stwarzają ograniczenia np. dla rozwoju e-commerce. Projektowane rozporządzenie ma zapewnić realizację zmiany tego stanu rzeczy, głownie poprzez:

1. Cyfryzację dokumentów i raportów fiskalnych,

2. Zapewnienie transmisji danych z kas do centralnego repozytorium,

3. Umożliwienie zaawansowanej analizy danych fiskalnych.

W rozporządzeniu określono nowe definicje i terminologię związane z przepisami rozporządzenia. W definicji dokumentów fiskalnych i niefiskalnych dopuszczono możliwość emitowania ich w postaci elektronicznej oraz transmitowania za pośrednictwem interfejsów komunikacyjnych do repozytorium lub repozytorium testowego. Repozytorium to system teleinformatyczny, prowadzony przez ministra właściwego do spraw finansów publicznych, którego jednym z celów funkcjonowania jest odbieranie danych przekazywanych przez kasy rejestrujące oraz komunikacja z kasami w zakresie niezbędnym do ich konfiguracji oraz realizowania innych zadań kontroli skarbowej. Repozytorium testowe jest systemem teleinformatycznym ułatwiającym producentom kas oraz innym firmom, zajmującym się ich obsługą, dokonywanie czynności serwisowych i konfiguracyjnych.

W treści definicji zdefiniowano także moduł kryptograficzny, którego zadaniem jest podpisywanie cyfrowe emitowanych dokumentów fiskalnych i niefiskalnych w taki sposób, że wygenerowany podpis jest umieszczany w treści dokumentu. Ujednolicono definicję producenta i podmiotów wprowadzających kasy do obrotu.

Rozporządzenie zawiera wyróżnienie rodzajów kas na względu na formę obrotu lub rejestracji sprzedaży towarów i usług. Ze względu na dopuszczenie emisji dokumentów fiskalnych lub niefiskalnych w postaci elektronicznej oraz komunikacji z zewnętrznymi systemami teleinformatycznymi oraz repozytorium i

repozytorium testowym kasa musi zawierać interfejsy zewnętrzne. Zestaw elementów kasy został także uzupełniony o wymóg posiadania przez kasę interfejsu komunikacyjnego do terminala płatniczego.

Rozporządzenie wiąże sposób zapisu dokumentów fiskalnych i niefiskalnych w postaci elektronicznej ze strukturami logicznymi określonymi w art. 193a ustawy Ordynacja podatkowa. Powoduje to powiazanie postaci elektronicznej dokumentów fiskalnych i niefiskalnych emitowanych przez kasę ze strukturami logicznymi jednolitego pliku kontrolnego.

Ponadto rozporządzenie wiąże ze sobą jednoznacznie i zapewnia zgodność danych na dokumentach fiskalnych i niefiskalnych emitowanych przez kasę oraz zapisanych w pamięci fiskalnej i w pamięci chronionej kasy. Podobne regulacje zostały zawarte odnośnie danych z rejestrów dobowych powiązanych z danymi wykazanymi na paragonach fiskalnych i rejestrach zdarzeń.

Rozporządzenie definiuje elementy paragonów fiskalnych emitowanych przez kasę w tym podpis cyfrowy paragonu przy użyciu klucza prywatnego kasy a także reguluje sposób przekazywania przez producenta kas kluczy publicznych do repozytorium.

Rozporządzenie mówi o potrzebie uzyskania nowego potwierdzenia (homologacji) w przypadku wprowadzenia zmian w konstrukcji, funkcjach i oprogramowaniu kasy przed ich wprowadzeniem do obrotu oraz definiuje zakres badań i zawartość sprawozdania z powyższych badań. Precyzyjne określenie jednoznacznych wymogów w zakresie homologacji znacząco przyspiesza ten proces i obniża jego koszty dla przedsiębiorców.

5.2.2 Opinia prawna Fundacji Panoptykon[2]

Fundacja Panoptykon, której celem jest działanie na rzecz wolności i ochrony praw człowieka w społeczeństwie nadzorowanym, sporządziła opinię prawną na temat projektu rozporządzenia Ministerstwa Rozwoju w sprawie kryteriów i warunków technicznych, którym muszą odpowiadać kasy rejestrujące w kontekście ochrony prywatności.

Autorzy wskazują, że projekt rozporządzenia w obecnym kształcie nie spełnia wymogów wynikających z Konstytucji RP, stanowi poważne zagrożenie dla autonomii jednostki i prawa do prywatności oraz może prowadzić do intensyfikacji nadzoru nad obywatelami, związanego z obowiązkami fiskalnymi.

Istotne zastrzeżenia prawników Fundacji Panoptykon budzi również pomysł utworzenia centralnego repozytorium transakcji. Podzielić należy ich pogląd, że takie repozytorium będzie zupełnie nową, pod względem jakościowym i ilościowym, bazą danych, która z punktu widzenia ochrony teleinformatycznej będzie bardzo cennym zasobem informacyjnym do zdobycia przez przestępców.

W opinii zwraca się też uwagę na fakt, że nie wiadomo, kto będzie administratorem repozytorium, kto i na jakich zasadach miałby dostęp do danych itd. Fundacja stwierdza: „bez jasnego i precyzyjnego określenia celu przetwarzania danych, nie można poprawnie przeprowadzić testu proporcjonalności tzn. ocenić czy wartości stojące za stworzeniem repozytorium mogą dawać podstawy dla ograniczenia prawa do ochrony danych osobowych i prawa do prywatności."

5.3 Kontekst Finansowy

Na pierwszy rzut oka kontekst finansowy może się wydawać wątkiem pobocznym w dyskusji na temat bezpieczeństwa teleinformatycznego i ochrony prywatności w szeroko rozumianym projekcie „e-paragon". Podkreślane publicznie są informacje dotyczące kosztów wymiany kas rejestrujących oraz zysk sektora publicznego wynikający z ograniczenia nielegalnego obrotu towarami i usługami. Rzadko jednak pojawia się aspekt wartości zagregowanych danych o transakcjach.

5.3.1 Wymiana kas rejestrujących

Projekt rozporządzenia Ministerstwa Rozwoju z 17 sierpnia 2016 r. w sprawie kryteriów i warunków technicznych, którym muszą odpowiadać kasy rejestrujące zakłada funkcjonowanie od 1 stycznia 2018 r. urządzeń obsługujących cyfryzację dokumentów i raportów fiskalnych oraz transmisję online danych z kas fiskalnych do centralnej bazy danych.

[2] https://panoptykon.org/sites/default/files/panoptykon_mr_uwagi_kasy_rejestrjace_13.09.2016.pdf

Koszt wymiany urządzeń jest szacowany różnie. Ministerstwo Rozwoju wskazuje kwotę ok. 700 mln zł[3]. Natomiast Polska Izba Handlu szacuje, że koszt może osiągnąć nawet 4 mld zł[4].

5.3.2 Ograniczenie „szarej strefy"

Głównym argumentem zwolenników koncepcji „e-paragon" jest możliwość otrzymywania danych z transakcji fiskalnych automatycznie, co 72 godziny, w postaci cyfrowej. Umożliwi to jednostkom kontrolującym budowę centralnej bazy danych (centralnego repozytorium paragonów) i zapewnienie sobie bardzo dużych możliwości analitycznych (po opracowaniu odpowiednich algorytmów i oprogramowania), dzięki którym zwiększy się liczba i efektywność kontroli przedsiębiorców. Resort szacuje, że w ten sposób do budżetu wpłynie ok 2 – 3 mld zł. więcej niż do tej pory.

5.3.3 Rzeczywista wartość danych z transakcji

Dane z transakcji i sposób ich przetwarzania w koncepcji „e-paragon" są cenne nie tylko z punktu widzenia fiskusa i większego prawdopodobieństwa kontroli skarbowej skutkującej nałożeniem kary lub zwiększenia świadomości tej kary wśród podatników. Istotnym elementem, a być może i najistotniejszym z punktu widzenia bezpieczeństwa całej koncepcji, jest ich wartość biznesowa.

Przedsiębiorcy, banki i wszyscy inni interesariusze, którzy już teraz mają dostęp do tych danych, korzystają z nich na potrzeby prowadzenia własnych działalności. Weryfikują zapasy towarów, profilują klientów, prowadzą akcje marketingowe itp.

Należy zwrócić uwagę, że o ile w pierwszych fazach projektu „e-paragon", obecnie dyskutowanych, przetwarzane dane będą zanonimizowane (tak jak jest to do tej pory, o ile nie korzysta się z programów lojalnościowych etc.) zarówno po stronie przedsiębiorcy jak i jednostek kontrolujących, to w wizjach najwyższego kierownictwa administracji publicznej, szczególnie po upowszechnieniu się obrotu bezgotówkowego, wśród tych danych mogą znaleźć się dane osobowe, w tym też wrażliwe (patrz: pomysły na wysyłanie e-paragonów na nr telefonu, adres poczty elektronicznej czy powiązanie ich z kontami płatniczymi). Wartość takich danych będzie ogromna, a ich niewłaściwe wykorzystanie może doprowadzić do wielu nadużyć wraz z całkowitą utratą prywatności.

5.4 Kontekst Społeczny

Zmiany w sposobie przetwarzania danych fiskalnych mogą mieć bardzo daleko posunięte konsekwencje społeczne oraz doprowadzić do zmian gospodarczych na różnych poziomach.

5.4.1 Ochrona prywatności

Dane o użytkownikach, konsumentach są coraz cenniejsze. Wartość mają wszystkie dane od adresu poczty elektronicznej, przez numery kart płatniczych, dane kontaktowe do danych konsumenckich. Zarówno zindywidualizowane jak i zbiorcze. Ochrona tego typu danych, pośrednio lub bezpośrednio, powiązanych z prywatnością użytkownika powinna być w dzisiejszych realiach jednym z priorytetów bezpieczeństwa jako działanie profilaktyczne, tym bardziej że podstawy daje sama ustawa zasadnicza – Konstytucja RP w rozdziale II - Wolności, prawa i obowiązki człowieka i obywatela. Art. 47. stanowi „Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym."

Warto również zwrócić uwagę na działania w zakresie bezpieczeństwa cyberprzestrzeni innych resortów. Ministerstwo Cyfryzacji w proponowanej Strategii Cyberbezpieczeństwa RP[5] na lata 2016 – 2020 w rozdziale 2. zatytułowanym poszanowanie praw i wolności w cyberprzestrzeni wskazuje „Wszelkie działania podejmowane przez rząd Rzeczypospolitej Polskiej w dziedzinie zwiększania cyberbezpieczeństwa będą się odbywały z poszanowaniem prawa i wolności obywateli. Rząd RP w pełni respektuje prawo do prywatności oraz stoi na stanowisku, że wolny i otwarty Internet jest bardzo istotnym elementem funkcjonowania dzisiejszego społeczeństwa.

---

[3] http://biznes.gazetaprawna.pl/artykuly/955606,e-paragon-tylko-w-sieci.html

[4] http://ksiegowosc.infor.pl/podatki/vat/kasy-fiskalne/746029,Wymiana-kas-fiskalnych-do-konca-2017-roku.html

[5] https://mc.gov.pl/files/strategia_v_29_09_2016.pdf

Cyberbezpieczeństwo nie może być zapewniane przez Państwo kosztem praw człowieka. Miarą cyberbezpieczeństwa jest nie tylko stopień zabezpieczenia i przeciwdziałanie zagrożeniom dla rozwoju sektora e-commerce, funkcjonowania e-państwa i infrastruktury krytycznej, ale także stopień zabezpieczenia swobodnego pozyskiwania informacji oraz ich przekazywania za pomocą sieci Internet, jak również stopień zabezpieczenia innych form realizacji praw podstawowych w cyberprzestrzeni."

Z punktu widzenia ochrony teleinformatycznej, systemy, w których przetwarzane są dane osobowe czy inne szczególnie istotne, są narażone na ataki dużo bardziej niż inne i projektując je należy mieć tego świadomość. Repozytorium danych z transakcji, nawet jeśli będzie przetwarzać tylko zanonimizowane dane konsumentów to i tak będzie jednym z najbardziej pożądanych przez przestępców zbiorów, przez co narażone będą na technologiczne ataki oraz naruszenia bezpieczeństwa spowodowane nadużyciem posiadanych uprawnień związanych z dostępem do tych danych[6].

5.4.2 Świadomość zagrożeń

Należy zwrócić uwagę na fakt, że społeczeństwo, nie tylko polskie, posiada bardzo małą świadomość na temat zagrożeń teleinformatycznych. Co więcej, nie zdaje sobie też sprawy, że udostępniając pewne dane o sobie, zgadza się de facto na ich przetwarzanie przez szereg powiązanych ze sobą przedsiębiorstw. Dlatego że niepokojem należy przyjąć brak przedstawiania w propozycjach do koncepcji „e-paragon" w wystarczający sposób aspektów bezpieczeństwa teleinformatycznego, szczególnie w najbardziej wrażliwych kwestiach (dalszy rozwój projektu, wymagania dla centralnego repozytorium paragonów etc.).

5.4.3 Błędy, nadużycia analityków

Nie są znane publicznie założenia na temat funkcjonowania centralnego repozytorium paragonów ani funkcji oprogramowania jakie będzie tam wykorzystywane. Należy jednak zdawać sobie sprawę, że błąd użytkownika bazy danych lub błąd aplikacji go wspomagającej może skutkować nieuzasadnioną kontrolą lub karą skarbową.

5.4.4 Małe przedsiębiorstwa

W opinii ekspertów zmianami związanymi z projektem „e-paragon" najbardziej dotknięte będą małe przedsiębiorstwa ze względu na krótki termin wymiany kas jak i sam jej koszt.

[6] jako przykład można podać niedawne doniesienia o nadużyciach związanych z dostępem do bazy PESEL: http://di.com.pl/komornicy-masowo-pobierali-dane-z-bazy-pesel-abw-prowadzi-sledztwo-55371

6 Zasady bezpieczeństwa teleinformatycznego w kontekście transakcji fiskalnych

Prawidłowo chroniony system teleinformatyczny powinien odznaczać się trzema cechami bezpieczeństwa:

- poufnością,
- integralnością,
- dostępnością.

Jest to jeden z najczęściej spotykanych modeli identyfikacji cech, dzięki którym można uznać system za zabezpieczony. W terminologii anglojęzycznej system określany jest jako CIA (Confidentiality, Integrity, Availability).

Cechy te oznaczają, że trzeba zapewnić, aby informacja w nim przetwarzana była traktowana poufnie, zgodnie z przyznanymi prawami dostępu, powinna ona zachować swoją integralność, tak aby można było uznać ją za wiarygodną i nie powinny występować problemy z dostępem do tej informacji dla osób mających odpowiednie uprawnienia.

Powyższe cechy dotyczą oprogramowania, sprzętu i procesów komunikacji między jednym i drugim.

Zagrożenia dla tak rozumianego modelu bezpieczeństwa interpretować należy jako:

- nieuprawniony dostęp do informacji i procesów jako naruszenie ich poufności,
- zmiana lub inne zakłócenie informacji i wykonywanych procesów jako naruszenie ich integralności,
- blokada dostępu do informacji i procesów jako naruszenie ich dostępności.[7]

Powyższe zasady zostały uwzględnione m.in. w Rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

6.1 Homologacja kas rejestrujących

Bez ważnej homologacji kas rejestrujących nie jest legalne ewidencjonowanie obrotu oraz kwot należnego podatku. W RP homologacji kas rejestrujących na wniosek ich producentów lub importerów dokonuje Główny Urząd Miar, który tym samym stanowi zaufaną stronę oraz ważne ogniwo w procesie zapewnienia także bezpieczeństwa teleinformatycznego transakcji fiskalnych.

Ważna homologacja potwierdza bowiem, że urządzenia we właściwy sposób raportują dane transakcyjne oraz przechowują informacje w sposób bezpieczny.

Warunkiem dopuszczenia stosowania kasy do ewidencjonowania jest również odpowiednie przechowywanie danych lub ich bezpieczny przekaz na zewnętrzne nośniki danych oraz unikatowy numer pamięci fiskalnej kasy. Niespełnienie tych wymogów skutkuje odmową wydania przez prezesa Głównego Urzędu Miar właściwego potwierdzenia, a w konsekwencji brakiem możliwości prowadzenia ewidencji za pomocą kasy.

Homologacja ma na celu potwierdzenie budowy kasy zgodnie z rozporządzeniem, a przez to zagwarantowanie dochowania staranności, że żadna z zasad (poufności, integralności i dostępności) nie jest złamana. Rozporządzenie dotyczące kas zapewnia bowiem poprzez wymagania techniczne, że kasa będzie chroniła i udostępniała autoryzowanym użytkownikom dane fiskalne przechowywane wewnątrz.

Brak homologacji dla urządzenia zdecydowanie zwiększa ryzyko ataku na poufność, integralność oraz dostępność danych i dlatego nie powinno się takich urządzeń dopuszczać do eksploatacji.

[7] http://rcb.gov.pl/wp-content/uploads/Załącznik-nr-1-do-NPOIK-2015.pdf

7 Badania

7.1 Metodyka

Badania Fundacji Bezpieczna Cyberprzestrzeń w zakresie bezpieczeństwa teleinformatycznego transakcji fiskalnych prowadzone były etapowo w dwóch obszarach.

Pierwszy dotyczył aspektów technicznych i objął swoim zakresem zapoznanie się z założeniami koncepcji „e-paragon" i dokumentów z nią związanych (przede wszystkim projekt rozporządzenia Ministerstwa Rozwoju w sprawie kryteriów i warunków technicznych, którym muszą odpowiadać kasy rejestrujące z dnia 17.08.2016 r.). Następnie przeprowadzenie spotkań konsultacyjnych z przedstawicielami administracji publicznej, producentów rozwiązań technologicznych oraz ze specjalistami ds. bezpieczeństwa teleinformatycznego. Dla wszystkich zainteresowanych stron zorganizowano debatę ekspercką. W dalszej kolejności, na podstawie zebranych informacji, dokonano identyfikacji i analizy ryzyka oraz przygotowano wnioski i rekomendacje.

Drugi obszar związany był z badaniem aspektu ochrony prywatności i gotowości grup społecznych na proponowane zmiany. W tym celu zlecono ogólnopolskie badania opinii społecznej oraz przeprowadzono podobne ankiety wśród specjalistów bezpieczeństwa teleinformatycznego.

Informacje niezbędne do pełnego zrozumienia proponowanych zmian przedstawiono w rozdziale „Kontekst".

7.1.1 Metodyka identyfikacji i analizy ryzyka

Dla zobrazowania szerokiego spektrum zagrożeń i opisania ich w systematyczny sposób posłużono się procesem identyfikacji i analizy ryzyka.

W opracowaniu nie zawarto etapu ewaluacji ryzyka, ponieważ określenie kryteriów ryzyka (poziomów odniesienia, względem których określa się istotność ryzyka, a z nimi z kolei porównuje się wynik analizy ryzyka[8]) stanowi odpowiedzialność osób decyzyjnych. Raport natomiast, dzięki wynikom badań opinii społeczeństwa polskiego i grupy specjalistów ds. bezpieczeństwa teleinformatycznego wskazuje, jakie poziom powinien być wzięty pod uwagę, a tym samym jakie ryzyko uznane za akceptowalne.

Poziom ryzyka oceniony został na podstawie szacunkowych wartości prawdopodobieństwa i następstw (skutków).

Prawdopodobieństwo zostało oszacowane na postawie poniższej skali jakościowej:

- Małe – brak informacji o zdarzeniach historycznych, brak przesłanek i podatności o możliwości wystąpienia zdarzenia;
- Średnie – zarejestrowano informacje o zdarzeniach historycznych, będących potencjalnymi źródłami ryzyka; istnieje możliwość wskazania przesłanek o możliwości wystąpienia zdarzenia;
- Duże – wystąpienie zdarzeń w przeszłości (udokumentowane, opisano dla tożsamych systemów, protokołów); zidentyfikowanie podatności bezpośrednio dla zdarzenia.

Następstwa zostały ocenione jako wpływ ryzyka bezpieczeństwo rozumiane jako wpływ ryzyka na poufność, dostępność, integralność danych oraz możliwość naruszenia prywatności (w zależności od charakteru danych):

- Niski – zdarzenie nie spowoduje żadnego wpływu na cechę bezpieczeństwa i proces przetwarzania danych;
- Średni – zdarzenie może okazać się niebezpieczne jeśli wystąpią dodatkowe okoliczności;
- Wysoki – zdarzenie wpływa bezpośrednio na cechę bezpieczeństwa i przerywa proces przetwarzania danych.

[8] Na podstawie normy PN-ISO 31000:2012

Poziom ryzyka określa się jako kombinację prawdopodobieństwa i największej wartości z 3 kategorii następstw, zgodnie z tabelą:

Prawdopodobieństwo		Następstwa (wpływ ryzyka)		
DUŻE 3		ISTOTNE	KRYTYCZNE	KRYTYCZNE
ŚREDNIE 2		ISTOTNE	ISTONE	KRYTYCZNE
MAŁE 1		SZCZĄTKOWE	ISTONE	ISTOTNE
		NISKI 1	ŚREDNI 2	Wysoki 2

Ryzyko szczątkowe interpretować należy jako ryzyko, którego nie można w łatwy sposób wyeliminować, koszty zabezpieczeń przewyższają zdecydowanie możliwe skutki i jest to ryzyko które można zaakceptować w działalności operacyjnej.

Ryzyko istotne rozumieć należy jako ryzyko, które trzeba brać pod uwagę w działalności i sukcesywnie wprowadzać kolejne środki je ograniczające.

Ryzyko krytyczne jest to ryzyko, które powinno zostać jak najszybciej wyeliminowane (ograniczone, zagospodarowane) w działalności systemów i organizacji, gdyż jego zmaterializowanie się doprowadzi do poważnych strat.

7.1.1.1 Definicje

Ryzyko – wpływ niepewności na cel

Identyfikacja ryzyka – proces wyszukiwania, rozpoznawania i opisywania ryzyka

Źródło ryzyka – element, który sam lub w połączeniu z innymi ma wewnętrzny potencjał, aby powodować powstanie ryzyka

Analiza ryzyka – proces dążący do poznania charakteru ryzyka oraz określenia poziomu ryzyka

Poziom ryzyka – wielkość ryzyka lub kombinacji ryzyka, wyrażona w postaci kombinacji następstw oraz ich prawdopodobieństwa

Kryteria ryzyka – poziomy odniesienia, względem których określa się ważność ryzyka

Ewaluacja ryzyka – proces porównywania wyników analizy ryzyka z kryteriami ryzyka w celu stwierdzenia, czy ryzyko jest i/lub jego wielkość są akceptowalne lub tolerowalne

7.2 Badanie własne w zakresie bezpieczeństwa teleinformatycznego wykorzystywanych urządzeń i technologii.

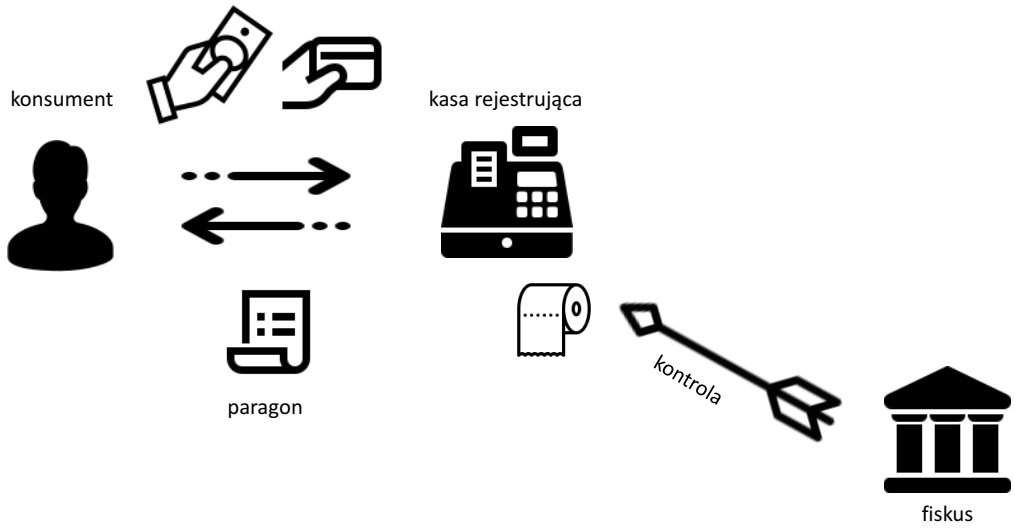
Niniejszy raport sporządzany jest w chwili, w której jedynym oficjalnym dokumentem traktującym o projekcie „e-paragon" jest projekt rozporządzenia Ministerstwa Rozwoju w sprawie kryteriów i warunków technicznych, którym muszą odpowiadać kasy rejestrujące z dnia 17 sierpnia 2016 r. (bez niektórych z wymienianych w projekcie załączników). Dodatkowo zapowiadane jest wydanie rozporządzenia opisującego wymagania dla repozytorium „e-paragonów".

Informacje dotyczące dalszego rozwoju projektu są zaczerpnięte i wnioskowane z informacji przedstawianych przez kierownictwo ministerstw w mediach i opinii eksperckich.

Generalnie można wyróżnić kilka modeli systemów: tych które funkcjonują, są planowane lub mogą być w przyszłości wdrożone (każdy z nich stanowi rozwinięcie poprzedniego):

- model stosowany obecnie
- model w roku 2018 przewidziany ww. rozporządzeniem
- model zintegrowanej kasy fiskalnej z terminalem płatniczym
- model z kasą fiskalną rozumianą jako oprogramowanie na dowolnej platformie sprzętowej
- model bez możliwości otrzymania przez konsumenta papierowej kopii paragonu

7.2.1 Model stosowany obecnie



Założenia:

Konsument: otrzymuje kopię papierową paragonu.

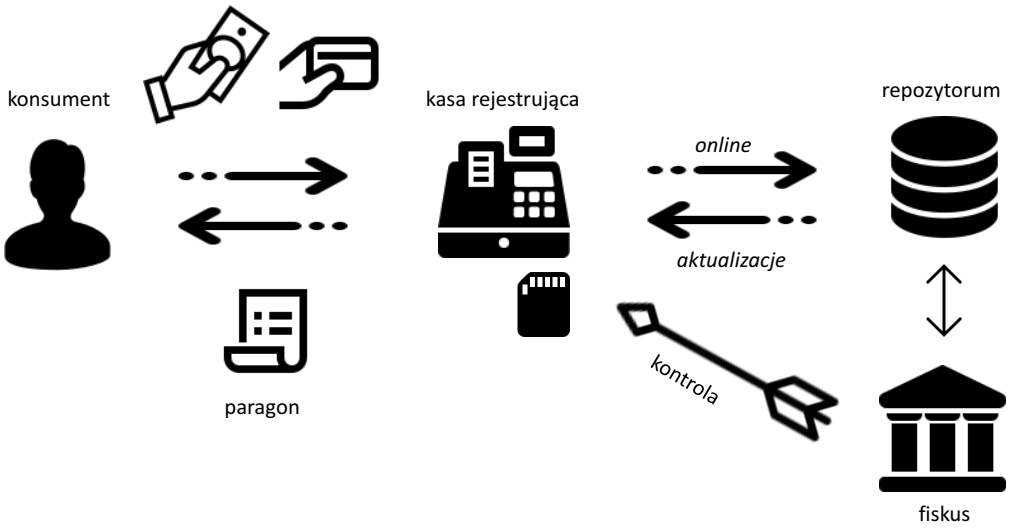
Podatnik: przechowuje kopię papierową lub elektroniczną paragonu (zależnie od typu posiadanego urządzenia) lokalnie. Dane są zanonimizowane.

Fiskus: nie dysponuje zbiorem danych o transakcjach u siebie. W celu kontroli żąda od podatnika okazania wskazanych dokumentów.

Opis:

Funkcjonujący obecnie system fiskalizacji jest uznawany za bezpieczny, a system homologacji weryfikujący bezpieczeństwo urządzeń fiskalnych ustandaryzowany. Dane są rozproszone. Brak centralnego systemu do analizy i kontroli transakcji sprzedaży, a systemy i urządzenia fiskalne są niedostosowane do realizacji centralnego raportowania transakcji.

7.2.2 Model podstawowy w roku 2018 przewidziany projektem rozporządzenia



Założenia:

Konsument: otrzymuje kopię papierową paragonu. Na swoje życzenie może gromadzić w systemie dane dotyczące jego transakcji.

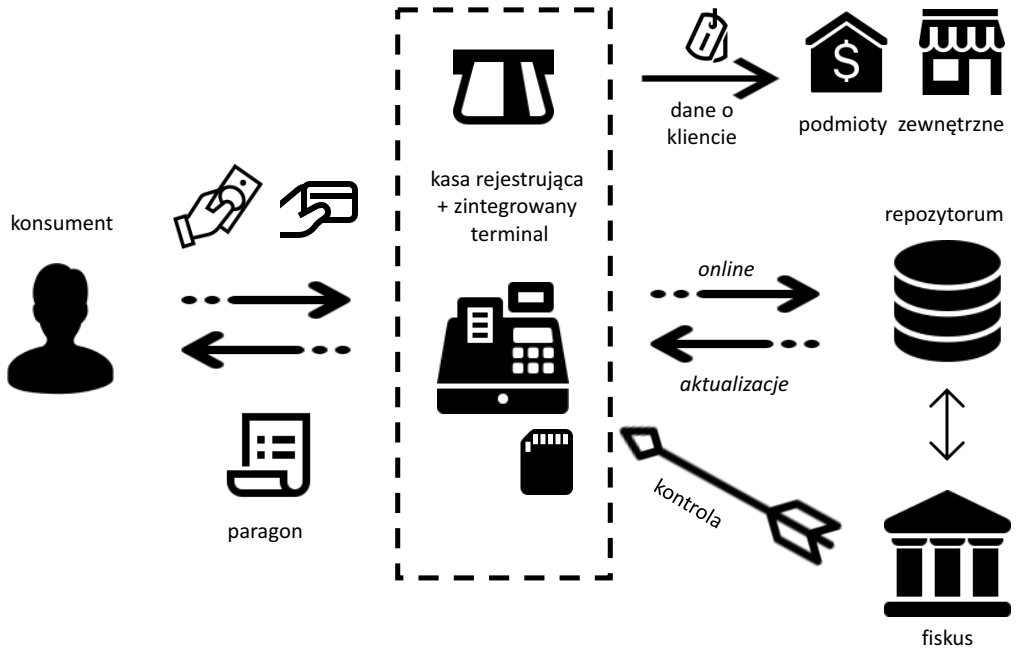
Podatnik: przesyłanie danych o każdej transakcji odbywa się w czasie rzeczywistym do repozytorium (docelowo ze względów technicznych – co 72 godziny).

Fiskus: dysponuje repozytorium agregującym dane i narzędziami analitycznymi zapewniającymi efektywność kontroli skarbowych.

Opis:

Utworzone zostaje centralne repozytorium i system do zaawansowanej analizy i kontroli transakcji sprzedaży. Systemy i urządzenia fiskalne zostają dostosowane do przesyłania danych przez Internet. Wprowadzone zostają standardy połączenia kas fiskalnych z centralnym repozytorium.

7.2.3 Model zintegrowanej kasy fiskalnej z terminalem płatniczym



Założenia:

Konsument: otrzymuje kopię papierową paragonu. Ma możliwość otrzymania paragonu w formie elektronicznej poprzez usługi zapewnianych przez interfejs z terminalem płatniczym. Na swoje życzenie może gromadzić w systemie dane dotyczące jego transakcji.

Podatnik: przesyłanie danych o każdej transakcji odbywa się w czasie rzeczywistym do repozytorium (założenie; docelowo ze względów technicznych – co 72 godziny). Dodatkowo poprzez terminal dane są przekazywane innym podmiotom (centra rozliczeniowe i banki)

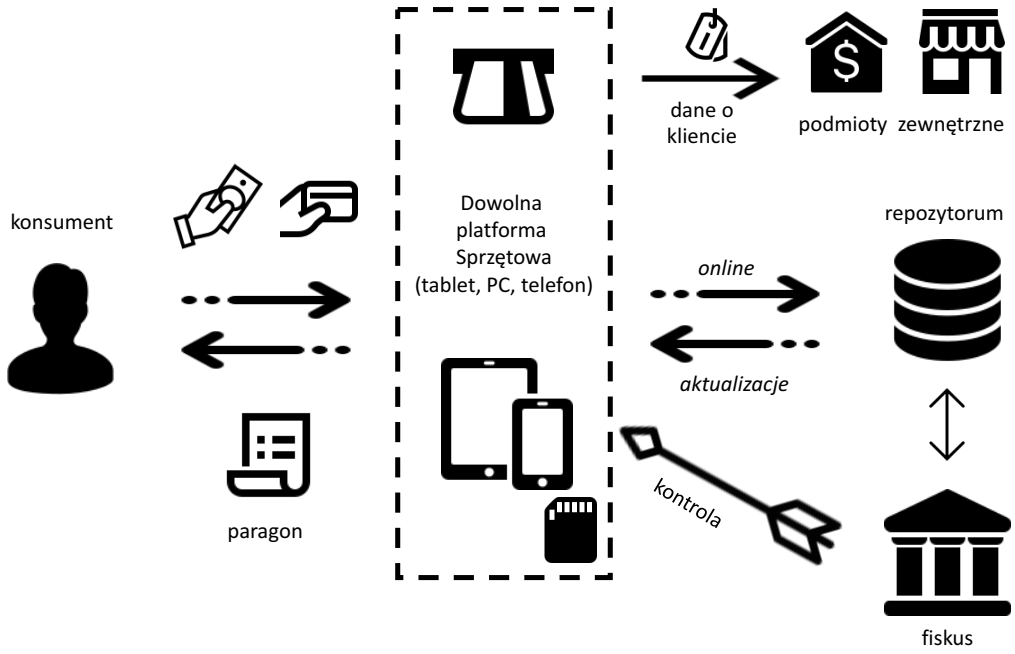
Fiskus: dysponuje repozytorium agregującym dane i narzędziami analitycznymi zapewniającymi efektywność kontroli skarbowych.

Bank (ogólnie instytucje finansowe i rozliczeniowe): dysponuje danymi zakupowymi klientów, których obsługuje. Docelowo nie tylko danymi standardowo zawartymi na paragonie.

Opis:

Zdaniem autorów rozwinięcia koncepcji „e-paragon", umożliwienie dostępu do danych kas fiskalnych przez terminale płatnicze umożliwi ich wykorzystanie przez banki i inne przedsiębiorstwa celem skierowana klientom dodatkowych usług (np. zarządzania wydatkami).

7.2.4 Model z kasą fiskalną rozumianą jako oprogramowanie na dowolnej platformie sprzętowej



Założenia:

Konsument: otrzymuje głównie paragon w postaci elektronicznej na wskazane przez siebie konto.

Podatnik: nie korzysta z kasy rejestrującej w postaci dedykowanego urządzenia. Wykorzystuje w zamian dowolna platformę sprzętową na której może działać homologowane oprogramowanie. Przesyłanie danych, tak jak w poprzednich modelach, o każdej transakcji odbywa się w czasie rzeczywistym do repozytorium (założenie; docelowo ze względów technicznych – co 72 godziny). Dodatkowo z danych korzystają inne podmioty (centra rozliczeniowe i banki) i aplikacje (zakłada się szerokie udostępnienie danych programistom).

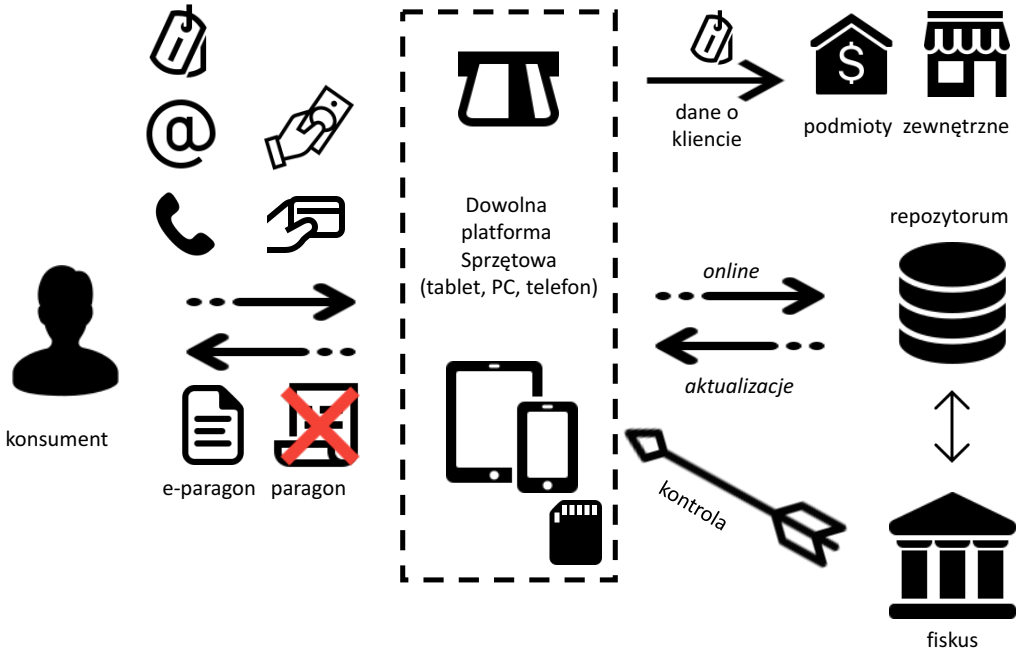
Fiskus: dysponuje repozytorium agregującym dane i narzędziami analitycznymi zapewniającymi efektywność kontroli skarbowych.

Bank (ogólnie instytucje finansowe i rozliczeniowe): dysponuje danymi zakupowymi klientów, których obsługuje. Docelowo nie tylko danymi standardowo zawartymi na paragonie.

Opis:

W dyskusjach nad rozwojem koncepcji „e-paragon" pojawia się model systemu (nieprzewidziany przez projekt rozporządzenia), w którym następuje całkowita rezygnacja z kas rejestrujących, rozumianych jako dedykowane urządzenia (hardware + software). W modelu tym, miałoby zastąpić je jedynie dedykowane oprogramowanie, które mogłoby być instalowane na powszechnie stosowanych platformach sprzętowych: telefonach, tabletach, terminalach itp.

7.2.5 Model bez możliwości otrzymania przez konsumenta papierowej kopii paragonu



Założenia:

Konsument: może otrzymać tylko wersję elektroniczną paragonu. Nawet przy płatności gotówkowej, obowiązek wydania potwierdzenia polega na podaniu danych zindywidualizowanego konta: poczty elektronicznej, lojalnościowego, czy choćby numeru telefonu. Na swoje życzenie może gromadzić w systemie dane dotyczące jego transakcji.

Podatnik i operator urządzenia: dysponuje pełnym (niezagregowanym i niezanonimizowanym) zasobem danych zakupowych.

Fiskus: dysponuje repozytorium agregującym dane i narzędziami analitycznymi zapewniającymi efektywność kontroli skarbowych.

Bank (ogólnie instytucje finansowe i rozliczeniowe): dysponuje danymi zakupowymi klientów, których obsługuje. Docelowo nie tylko danymi standardowo zawartymi na paragonie.

Opis:

Model zakłada całkowitą rezygnację z wersji papierowej kopii paragonu dla klienta. W związku z obowiązkiem wypełnienia powinności przekazania konsumentowi dokumentu potwierdzającego transakcję, będzie on musiał przedstawić podatnikowi wybraną przez siebie (i dostępną u podatnika) metodę przesłania e-paragonu. Najczęściej mówi się o wykorzystaniu adresu poczty elektronicznej, wiadomości tekstowej na wskazany numer abonenta lub programie lojalnościowym.

7.2.6 Szacowanie ryzyka

7.2.6.1 Charakterystyka incydentów

Aby odpowiednio zabezpieczyć systemy teleinformatyczne należy zrozumieć kim są i jakie motywacje mają osoby dokonujące włamań do systemów. Najczęściej spotykaną ich systematyką jest przedstawienie w trzech grupach:

1. Cyberprzestępcy, których główną motywacją działania jest chęć zysku finansowego. Nie jest dla nich istotne kto padnie ofiarą ich aktywności. Zwykle szukają jak najprostszych metod uzyskania korzyści majątkowej – eksplorują najsłabiej zabezpieczone systemy.
2. Haktywiści, czyli osoby które wykorzystują swoje umiejętności przede wszystkim w celach politycznych i społecznych. Nie jest celem ich działania bezpośrednia korzyść finansowa.
3. Grupy „sponsorowane" przez rządy obcych państw, których cele ataków są skrupulatnie wybierane i głównie ukierunkowane na pozyskanie jak największej ilości informacji (szpiegostwo) lub spowodowanie poważnych zakłóceń funkcjonowania innych państw (poprzez działania dezinformacyjne lub ataki na infrastrukturę krytyczną).

Biorąc pod uwagę dane, które mogą być przetwarzane w proponowanym systemie, trzeba podkreślić, że będą one cenne zarówno dla zwykłych cyberprzestępców jak i grup sponsorowanych. Dodatkowo haktywiści mogą wykorzystywać możliwość przełamania zabezpieczeń do dyskredytacji służb państwowych odpowiedzialnych za ich zabezpieczenie.

7.2.6.1.1 RAM scraping[9]

RAM scraping jest to nazwa techniki wykorzystywanej przez złośliwe oprogramowanie. Teoria zakłada uaktywnienie się takiego oprogramowania w momencie ładowania do pamięci RAM (random-access memory – pamięć obsługująca aktualnie wykonywane programy i potrzebne do nich dane) odpowiednich informacji, ich przechwycenie i przesłanie dalej – do atakujących. Technika jest o tyle użyteczna, że wykorzystuje słabość systemów obsługujących w pamięci RAM zdeszyfrowane informacje (dane są na bardzo krótki czas rozszyfrowywane, przetwarzane i znów szyfrowane). Jeśli przestępca wykorzystując podatności systemów sklepowych dostanie się do lokalnego serwera (do lokalnych sieci) może też uzyskać dostęp do systemów płatniczych i urządzeń z nim związanych. Podłączenie do sieci Internet systemów sklepowych multiplikuje wielokrotnie prawdopodobieństwo włamania.

Ten wektor ataku był wykorzystywany w przeszłości i doprowadził do jednych z największych wycieków danych[10]. Np. wyciek 40 mln danych kart płatniczych sieć Target kosztował ok. 236 mln USD.

7.2.6.1.2 Nieautoryzowany fizyczny dostęp do urządzeń

Uzyskanie fizycznego dostępu do urządzeń i systemów często oznacza również (posiadając odpowiednie umiejętności) uzyskanie dostępu do samych procesów i usług wykonywanych przez tą infrastrukturę. Dlatego też odpowiednie zabezpieczenie fizyczne jest istotne z punktu widzenia bezpieczeństwa teleinformatycznego. Dotyczy to zarówno pojedynczych elementów urządzeń (np. pamięci), jak i samych urządzeń (obudowy), pomieszczeń je przechowywujących (serwerownie, centra kontroli, mantrami), ale też i całych budynków (centra przetwarzania danych).

Na każdym poziomie stosowane powinny być adekwatne środki ochrony. Od zintegrowania modułów z urządzeniem (w kasach rejestrujących np. jest to zalanie modułu pamięci żywicą), przez zaplombowanie urządzenia i zabezpieczenia antykradzieżowe (podmiana terminali płatniczych to jedna z najprostszych metod uzyskania poufnych danych) do odpowiedniego zabezpieczenia centrów przetwarzania danych (zabezpieczenia perymetryczne, system kontroli dostępu, nadzór wizyjny etc.).

7.2.6.1.3 Awarie sprzętu

Każde urządzenie jest awaryjne i ma określoną żywotność. Konsekwencje awarii sprzętu informatycznego są znane osobom odpowiedzialnym za utrzymanie zasobów IT i prowadzą poprzez zatrzymanie działalności operacyjnej do strat finansowych i wizerunkowych. Dlatego też stale dokonuje się modernizacji

[9] http://artemonsecurity.com/20140116_POS_Malware_Technical_Analysis.pdf
[10] http://www.databreachtoday.com/target-breach-by-numbers-a-7205

infrastruktury IT, zapewnia odpowiednią redundancję sprzętu oraz utrzymuje się poziom niezawodności na stałym, określonym poziomie.

Utrzymanie ciągłości działania usługi po awarii sprzętu powinno być priorytetem każdego systemu.

7.2.6.1.4 Awarie łączy telekomunikacyjnych

Rozbudowane systemy teleinformatyczne korzystają z danych przetwarzanych w różnych lokalizacjach w związku z czym niezbędne stają się odpowiednie kanały przesyłania informacji (dostęp do sieci) Większość z nich jest obsługiwana przez zewnętrzne podmioty – np. dostawców usług internetowych. Należy zdawać sobie sprawę, że oni również mogą swojej usługi nie dostarczyć. Mogą paść ofiarą cyberataku lub klęski żywiołowej.

7.2.6.1.5 Błędy oprogramowania

Nawet najlepsze oprogramowanie, wielokrotnie testowane, zawierające rozbudowaną obsługę błędów i wyjątków, może zadziałać w sposób nieprzewidziany przez programistę. Usterki programów komputerowych powodujących ich nieprawidłowe działanie, wynikające z błędów deweloperów przy tworzeniu kodu źródłowego należy brać pod uwagę, a ich ryzyko będzie rosło odwrotnie proporcjonalnie do liczby audytów kodu, testów itp. (w przypadku kas rejestrujących oprogramowanie podlega homologacji Głównego Urzędu Miar). W środowiskach otwartych istnieje dodatkowe ryzyko nieprzewidzianego współdziałania oprogramowania z innymi aplikacjami.

7.2.6.1.6 Przechwytywanie komunikacji

Dane można uzyskać nie tylko poprzez dostęp do systemów, w których są przechowywane, ale także w momencie ich przesyłania pomiędzy urządzeniami. Jeśli dane są przesyłane w sposób jawny (niezaszyfrowany) ich odczytanie przy wykorzystaniu podstawowych narzędzi nasłuchujących (sniffing) jest banalnie proste. Dlatego w ostatnich latach popularność w powszechnym użyciu zdobyły szyfrowane wersje protokołów komunikacyjnych i samo szyfrowanie danych. Obecnie, z punktu widzenia bezpieczeństwa, biorąc pod uwagę możliwości obecnych systemów liczących, najnowsze algorytmy można uznać za tak bezpieczne, jak bezpieczne są klucze szyfrujące do nich użyte (długość, przechowywanie).

7.2.6.1.7 Atak DDoS

DDoS (ang. Distributed Denial of Service – rozproszona odmowa usługi) – atak na system komputerowy lub usługę sieciową w celu uniemożliwienia dostarczania swoich usług przeprowadzany równocześnie z wielu komputerów.

Istnieją trzy strategie, które są wykorzystywane do zablokowania działania strony internetowej, serwera lub infrastruktury:

- Przepustowość: kategoria ataku polegającego na wykorzystaniu zasobów sieciowych serwera. Serwer jest niedostępny.
- Zasoby: kategoria ataku polegającego na wykorzystaniu zasobów systemu maszyny i zablokowaniu przekazywania odpowiedzi na poprawne zapytania.
- Wykorzystanie błędu w oprogramowaniu: atak o nazwie "exploit", który wykorzystuje błąd w oprogramowaniu do zablokowania maszyny lub do przejęcia kontroli nad maszyną.

Trzecia strategia jest dużo łatwiejsza do przeprowadzenia w otwartym, powszechnie znanym środowisku, a trudna do realizacji w środowisku zamkniętym znanym tylko producentowi. (Środowisko otwarte to np. system operacyjny Android i aplikacja z funkcjami kasy (e-kasa), środowisko zamknięte to dedykowane systemy zaszyte w kasach fiskalnych w ich obecnym znaczeniu.)

7.2.6.1.8 Masowe wycieki danych

Wycieki danych są nieuniknione. Systemy stają się coraz bardziej złożone i konfigurowane w sposób mający zapewnić ich jak największą efektywność i interoperacyjność. Nierzadko kosztem bezpieczeństwa. Centralne bazy danych z wartościowymi informacjami są naturalnym celem przestępców. Wycieki takie przez lata mogą nie być upublicznianie. Dane w pierwszej kolejności sprzedawane są w zaufanym, hermetycznym gronie świata przestępczego i często, dopiero po latach, z uwagi na utratę w czasie ich wartości są publikowane.

7.2.6.1.9 Nieuprawnione wykorzystanie informacji

Jako nieuprawnione wykorzystanie informacji rozumie się w niniejszym raporcie wykorzystanie danych przez osoby posiadające autoryzowany dostęp do systemów je przetwarzających lecz niezgodnie z ich kompetencjami i obowiązkami. W przypadku koncepcji „e-paragon" będzie to oznaczało ryzyko nadużyć organów kontrolujących i przechowujących dane (np. banki), działania wbrew intencjom użytkowników dane przekazujących itp.

7.2.6.1.10 Szpiegostwo

Zdawać należy sobie sprawę, że centralna baza danych, zawierająca całość informacji o transakcjach w Polsce, przedsiębiorcach, a może się okazać, że i konsumentach, będzie nie tylko cenna jako zasób komercyjny, ale także jako podstawowe źródło informacji dla wywiadów gospodarczych, które, jeśli uda im się uzyskać dostęp, będą miały możliwość do prowadzenia skutecznych działań ekonomicznych i informacyjnych, o zwykłym szantażu nie wspominając.

7.2.6.1.11 Błędy konfiguracji urządzeń

Konfiguracja urządzeń, przyznawanie praw dostępu, czy rozumiane nieco szerzej zarządzanie regułami bezpieczeństwa, jest podstawowym obowiązkiem specjalistów zarządzających bezpieczeństwem systemów informatycznych. Ich prawidłowa realizacja zależy bezpośrednio od kompetencji i doświadczenia personelu. Dużo łatwiej jest błędnie skonfigurować otwarty system czy oprogramowanie niż system zamknięty, skonfigurowany przez producenta, pozostawiający użytkownikowi końcowemu jedynie możliwość definiowania parametrów nie wpływających na poziom bezpieczeństwa.

7.2.6.1.12 Phishing

Phishing jest to metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję, w celu wyłudzenia określonych informacji (np. danych logowania, szczegółów karty kredytowej) lub nakłonienia ofiary do określonych działań. Jest to rodzaj ataku opartego na inżynierii społecznej.[11] Najczęściej atak phishingowy przeprowadzany jest za pośrednictwem poczty elektronicznej. Ich celem są użytkownicy systemów posiadających istotne uprawnienia lub dane.

7.2.6.1.13 Wykorzystanie podatności

Każde z wymienionych powyżej zagrożeń wykorzystuje szeroko rozumiane podatności systemów informatycznych, czy to ludzkie czy techniczne. Jednak w związku z tym, że w koncepcji „e-paragon" może dojść do sytuacji, w której oprogramowanie rejestrujące i wyliczające należności podatkowe, będzie mogło być instalowane na dowolnej platformie sprzętowej (bezpośrednio nie określonej) – nie sposób wskazać wszystkich podatności. Dlatego też, w ostatnim modelu systemu („Model z kasą fiskalną rozumianą jako oprogramowanie na dowolnej platformie sprzętowej") w analizie ryzyka posłużono się tak ogólnie sformułowanym zagrożeniem. Jest ono w swojej istocie jednym z najgroźniejszych, ponieważ właśnie określenie konkretnej platformy sprzętowej, wymagań dla dedykowanych urządzeń i oprogramowania, powinno być punktem wyjścia do projektowania bezpiecznego systemu, gwarantującego poufność, integralność i dostępność danych z transakcji.

[11] https://pl.wikipedia.org/wiki/Phishing

ryzyko		skutki			
	prawdopodob.	poufność	integralność	dostępność	Poziom ryzyka
kasa rejestrująca:					
malware: ataki wykorzystujące technikę RAM scraping	1	3	1	1	3
nieautoryzowane fizyczne uzyskanie dostępu do urządzenia przetwarzającego dane	2	3	2	2	6
awarie sprzętowe	1	1	2	3	3
awarie łącza	3	1	2	2	6
błędy oprogramowania	2	2	2	2	4
terminal:					
przechwytywanie komunikacji terminalem a kasą	1	3	1	2	3
malware: ataki wykorzystujące technikę RAM scraping	3	3	1	1	9
przechwytywanie komunikacji poza systemem kasa-terminal	3	3	1	1	9
atak typu DDoS (na dostępność systemu),	3	1	1	3	9
nieautoryzowane fizyczne uzyskanie dostępu do urządzenia przetwarzającego dane	3	3	3	2	9
awarie sprzętowe	1	1	2	3	3
awarie łącza	3	1	2	3	9
błędy oprogramowania	2	2	2	2	4
repozytorium:					
atak typu DDoS (na dostępność systemu),	2	1	2	3	6
przechwytywanie komunikacji kasa – repozytorium	1	3	1	1	3
wyciek danych	3	3	1	1	9
nieuprawnione wykorzystanie informacji	3	3	1	1	9
nieautoryzowane fizyczne uzyskanie dostępu do urządzenia przetwarzającego dane	2	2	2	2	4
awarie sprzętowe	1	1	2	3	3
awarie łącza	2	1	2	3	6
błędy oprogramowania	1	2	2	2	2
naruszenie procedur bezpieczeństwa	2	3	2	2	6
ataki phishingowe na obsługę repozytorium	3	2	1	1	6
szpiegostwo	3	2	1	1	6
błędy konfiguracji urządzeń	2	2	2	2	4
inne platformy sprzętowe:					
wykorzystanie podatności innych platform sprzętowych	2	2	2	2	4

Komentarz:

Wraz z rozwojem koncepcji „e-paragon", siłą rzeczy, rozwijać i rozbudowywać będzie się system teleinformatyczny ją obsługujący. Integrowane będą kolejne urządzenia i dodawane funkcjonalności co będzie oznaczało wprost proporcjonalny wzrost liczby podatności systemu. Dodatkowo dane w każdym kolejnym etapie będą coraz bardziej wrażliwe i cenne dla przestępców przez co będzie rosła motywacja ich pozyskania.

7.3 Debata ekspercka

14 września 2016 r. Fundacja Bezpieczna Cyberprzestrzeń w ramach konferencji Security Case Study 2016 zorganizowała debatę ekspercką poświęconą w całości bezpieczeństwu teleinformatycznemu transakcji fiskalnych. Celem spotkania było szczegółowe poznanie koncepcji i pomysłów administracji na wdrożenie nowych technologii na rynku fiskalnym. Jednocześnie debata dawała możliwość wyartykułowania zainteresowanym stronom (m. in. przedstawicielom producentów rozwiązań technologicznych) swoich komentarzy, uwag oraz wątpliwości. Do rozmów zaproszono:

1. Ministerstwo Rozwoju
2. Ministerstwo Finansów
3. Ministerstwo Cyfryzacji
4. Główny Urząd Miar
5. Komitet Agentów Rozliczeniowych Związku Banków Polskich
6. Krajową Izbę Gospodarczą Elektroniki i Telekomunikacji
7. Polską Organizację Handlu i Dystrybucji
8. Konfederację Lewiatan
9. Fundację Rozwoju Obrotu Bezgotówkowego
10. Firmę Enigma Sp. z o. o.
11. Firmę Krypton Polska Sp. z o. o.

Ministerstwo Rozwoju, Ministerstwo Finansów oraz Główny Urząd Miar zrezygnowali z uczestnictwa w debacie. Firma Enigma Sp. z o.o. nie odpowiedziała na zaproszenie. Pozostali uczestnicy podzielili się swoją wiedzą i poglądami dot. bezpieczeństwa transakcji fiskalnych.

7.3.1 Przebieg

W związku z absencją Ministerstw Rozwoju i Finansów, pomimo usilnych starań organizatorów o udział jego przedstawicieli, niemożliwe było poznanie szczegółowych planów przedmiotowych resortów w kontekście szeroko rozumianego projektu „E-paragon". Uczestnicy musieli zatem oprzeć się na bieżącej wiedzy i medialnych informacjach (np. wywiadów z najwyższym kierownictwem Ministerstw) i na tej podstawie przewidywać i opiniować pomysły wiodących organów. Każdy z uczestników otrzymał możliwość swobodnej wypowiedzi oraz ustosunkowywania się do opinii interlokutorów, z którymi się nie zgadzał.

7.3.2 Stanowiska

By nie nadinterpretować stanowisk poszczególnych uczestników debaty oraz pozostając w sferze dyskusji natury merytorycznej w niniejszym zestawieniu celowo pominięto atrybucję poszczególnych, prezentowanych stanowisk, a skupiono się na istocie problemu – bezpieczeństwie i ochronie danych. Poglądy zgrupowano tematycznie.

7.3.2.1 Wartość przetwarzanych danych

- Uczestnicy debaty wyrazili wątpliwości co jest głównym celem proponowanych zmian: czy rzeczywiście uszczelnienie systemu podatkowego czy pozyskanie szczegółowych informacji o transakcjach, tym bardziej, że większość obserwowanych oszustw podatkowych dotyczy transakcji pomiędzy pomiotami gospodarczymi (B2B) a nie pomiędzy podmiotem a klientem indywidualnym (B2C). Zauważono jednak, że oficjalne stanowisko Ministerstwa Rozwoju i Ministerstwa Finansów, główny nacisk kładzie na zwiększenie ściągalności podatków.
- Zwrócono uwagę, że dane z transakcji to także dokumenty mogące stanowić dowód sądowy oraz same w sobie są wartością komercyjną.

7.3.2.2 Przesyłanie danych

- Podkreślono, że uzyskanie zdolności to przesyłania danych w czasie rzeczywistym będzie niemożliwe do zrealizowania. Dane będą agregowane lokalnie i zgodnie z harmonogramem przesyłane do repozytorium prawdopodobnie co 72 godziny. Operator repozytorium będzie miał możliwość jednak wmuszenia transferu danych w dowolnym momencie. Również producenci będą mieli dostęp do kas w celu przeprowadzania

aktualizacji oprogramowania. Bezpieczeństwo danych podczas transferu nie powinno być zagrożone, ponieważ projekt zakłada wykorzystanie mechanizmów kryptograficznych.

7.3.2.3 Centralne Repozytorium Danych

- Zgodzono się, że bezpieczeństwo centralnego repozytorium będzie kluczowe dla bezpieczeństwa całego systemu.
- Istotne będzie jakie dane będą przekazywane do repozytorium w kolejnych etapach rozwoju projektu „e-paragon"

7.3.2.4 Integracja kas fiskalnych z terminalami płatniczymi

- Znaczącą część czasu debaty poświęcono możliwościom integracji kas fiskalnych z terminalami płatniczymi, która może się okazać jednym z najbardziej podatnych na potencjalne zagrożenia obszarów. Słabości te wynikają z dwóch faktów: mniej rygorystycznych wymagań w zakresie bezpieczeństwa dla terminali płatniczych niż dla kas rejestrujących oraz przejmowania przez terminale funkcji kas lub uzyskiwanie dostępu do danych z kas. Rozwiązanie takie daje np. możliwości dostępu do informacji fiskalnych przez interfejs terminala lub np. możliwość zdalnego wydruku na kasie.
- Porównywano również same zabezpieczenia techniczne urządzeń dedykowanych rozliczeniom fiskalnym (kasy), w których zabezpieczenia są stosowane w warstwie sprzętowej jak i aplikacyjnej do urządzeń spełniających inne funkcje, ale mogących realizować także operacje „fiskalne" dzięki odpowiedniemu oprogramowaniu (terminale, telefony).
- Opracowanie odpowiedniej platformy sprzętowej uznano jako jeden z głównych czynników decydujących o bezpieczeństwie danych w całym systemie. Wskazanie w projekcie rozporządzenia na wysokie standardy modułów kryptograficznych (TPM 2.0 lub FIPS 140-2 lev. 2) uznano za wystarczające.

7.3.2.5 Koszt i charakter zmian

- W odniesieniu do aspektów ekonomicznych stanowisko większości uczestników było po stronie przedsiębiorców tzn., że powinni oni ponieść jak najmniejsze koszty związane ze zmianami. Mogło by się to odbyć poprzez wydłużenie możliwości korzystania z zakupionych do tej pory kas. Podkreślono również, że Państwo powinno wprowadzić więcej zachęt w postaci różnego rodzaju bonifikat.
- W zdecydowanej większości z aprobatą przyjęto rolę Głównego Urzędu Miar jako jednostki homologacyjnej zarówno sprzęt jak i oprogramowanie.

7.3.2.6 Obrót bezgotówkowy

- Uczestnicy debaty podkreślili, że zauważalny jest trend zmian dążący do jak najpowszechniejszego korzystania z transakcji bezgotówkowych. Projekt „e-paragon" się w niego wpisuje.
- Zauważono, że całkowite przejście na obrót bezgotówkowy jest jednak obecnie nierealne i jest to raczej możliwe w dalekiej przyszłości, a obrót bezgotówkowy jest podstawą dla rozwinięcia koncepcji „e-paragonu", w przeciwnym razie płacąc gotówką konieczne byłyby inne mechanizmy uwierzytelnienia płacącego.

7.3.2.7 Prywatność

- Zaznaczono, że nawet jeśli konsumenci będą zrzekać się swojej prywatności, korzystając czy to z płatności bezgotówkowych czy programów lojalnościowych to należy zrobić wszystko by ich decyzja była w pełni świadoma – konsument powinien być świadomy konsekwencji.
- Równocześnie poddano w wątpliwość opłacalność uszczelniania systemu podatkowego kosztem potencjalnej utraty prywatności konsumentów.

7.4 Wyniki badań społecznych

W celu określenia oczekiwań obywateli, poziomu ich świadomości o zagrożeniach oraz poglądów na temat proponowanych zmian zlecono badania sondażowe, na reprezentatywnej dla polskiego społeczeństwa grupie, dotyczące opinii na temat bezpieczeństwa danych i przetwarzania ich przez podmioty państwowe: „Postawy Polaków Wobec E-Paragonów".

7.4.1 Metodyka badania

Badanie zrealizowane zostało metodą CAWI (wywiady online), na próbie 1072 Polaków w wieku 17-60 lat, reprezentatywnej w stosunku do rozkładu płci, wieku i miejsca zamieszkania.

Dodatkowo zastosowana została waga analityczna, aby przybliżyć rozkład prośby do populacji pod względem wykształcenia i statusu zawodowego.

Badanie zrealizowane na zostało przez instytut badawczy Ipsos w dniach 26 – 30 sierpnia 2016 r. Do istotnych okoliczności badania zaliczyć należy fakt realizacji badania w okresie po pojawieniu się informacji o możliwym wycieku danych z bazy PESEL przez kancelarie komornicze, przed szerokim rozpowszechnieniem sprostowania i wyjaśnień przez instytucje publiczne.

Badanie składała się z 8 pytań zamkniętych z odpowiedziami w skali 1 - 4 (zdecydowanie tak / raczej tak / raczej nie / zdecydowanie nie) oraz jednego uzupełniającego pytania otwartego.

7.4.2 Cel badania

Określenie dominujących w społeczeństwie postaw wobec elektronicznych paragonów w kontekście gromadzenia przez Państwo danych zakupowych w powiązaniu z danymi osobowymi.

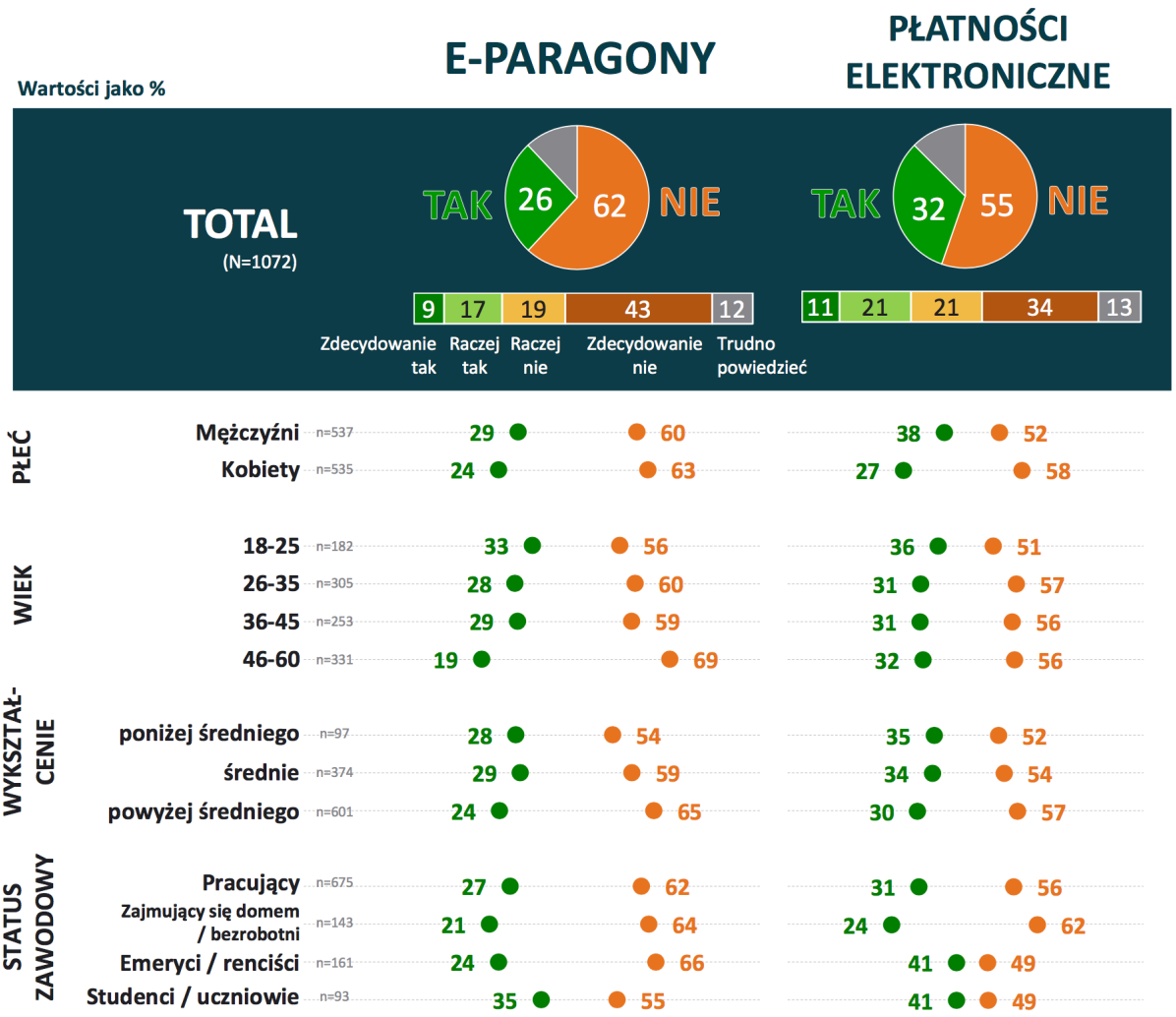
7.4.3 Wyniki badania

7.4.4 Poparcie dla przejścia na paragony elektroniczne i transakcje elektroniczne

Czy wiedząc, że paragony elektroniczne będą powiązane z Pana(i) danymi, chciał(a)by Pan(i) całkowicie zamienić:

1) tradycyjny paragon na paragon elektroniczny, który byłby wysyłany np. na Pana/Pani adres mailowy podawany sprzedawcy?

2) płatności gotówkowe na płatności elektroniczne? (np. płatności kartą płatniczą, telefonem *komórkowym itp.)*



Ponad połowa respondentów przeciwna jest zarówno przejściu na e-paragony, jak i całkowitemu zastąpieniu tradycyjnych płatności płatnościami elektronicznymi.

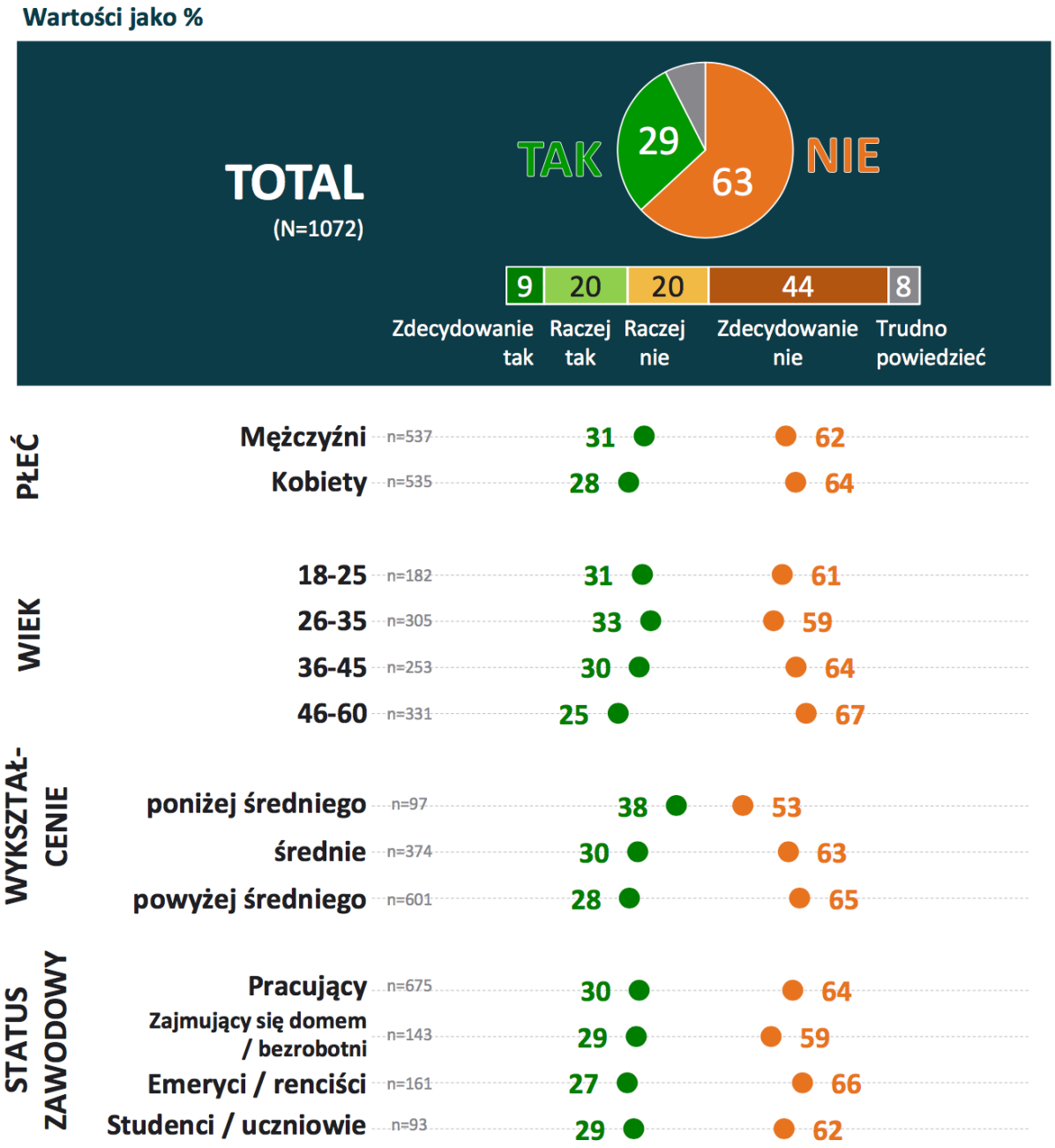
Za e-paragonami opowiada się niewiele ponad 1/4 ankietowanych.

Nieco większy odsetek zwolenników e-paragonów jest wśród osób młodszych – do 25 roku życia (33%). W najstarszej grupie respondentów sprzeciw wobec e-paragonów jest najsilniejszy – blisko 7 na 10 osób w wieku powyżej 45 lat opowiada się przeciwko nim.

Skłonność do poparcia zarówno dla e-paragonów, jak i zastąpienia wszystkich transakcji elektronicznymi jest tym niższa, im wyższe jest wykształcenie respondentów.

7.4.5 Zgoda na gromadzenie danych o zakupach przez Państwo

Czy wyraził(a)by Pan(i) zgodę na gromadzenie przez Państwo danych o wszystkich Pana/i zakupach?



Blisko 2/3 respondentów jest przeciwnych gromadzeniu przez Państwo danych o wszystkich ich zakupach, w tym blisko połowa (44%) wyraziła zdecydowany sprzeciw. Zgodę deklaruje niecałe 30% badanych.

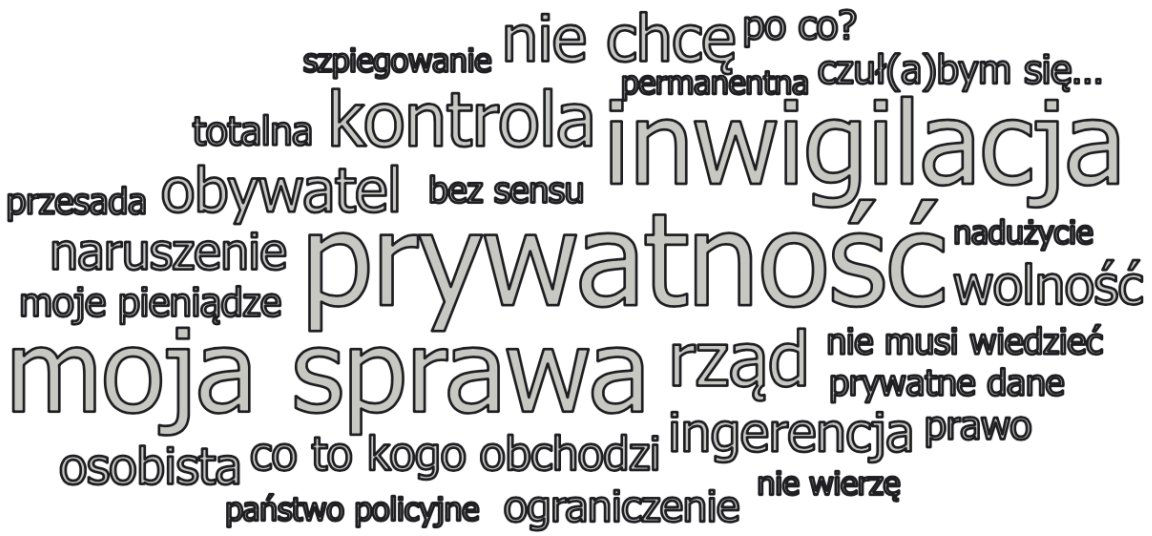
Najbardziej przychylni gromadzeniu przez Państwo danych zakupowych byli respondenci w wieku 26-35 lat – co trzeci wyraziłby na to zgodę. Respondenci powyżej 46 lat najczęściej wyrażali sprzeciw. Przeciwni byli zwłaszcza respondenci z wykształceniem wyższym, a najczęściej za – osoby o wykształceniu poniżej średniego.

7.4.5.1 Przyczyny niechęci do gromadzenia przez Państwo danych o zakupach

Dlaczego nie wyraził(a)by Pan(i) zgody na gromadzenie przez Państwo danych o wszystkich Pana/i zakupach i wydatkach?

Wartości jako %

SŁOWA KLUCZOWE W WYPOWIEDZIACH*

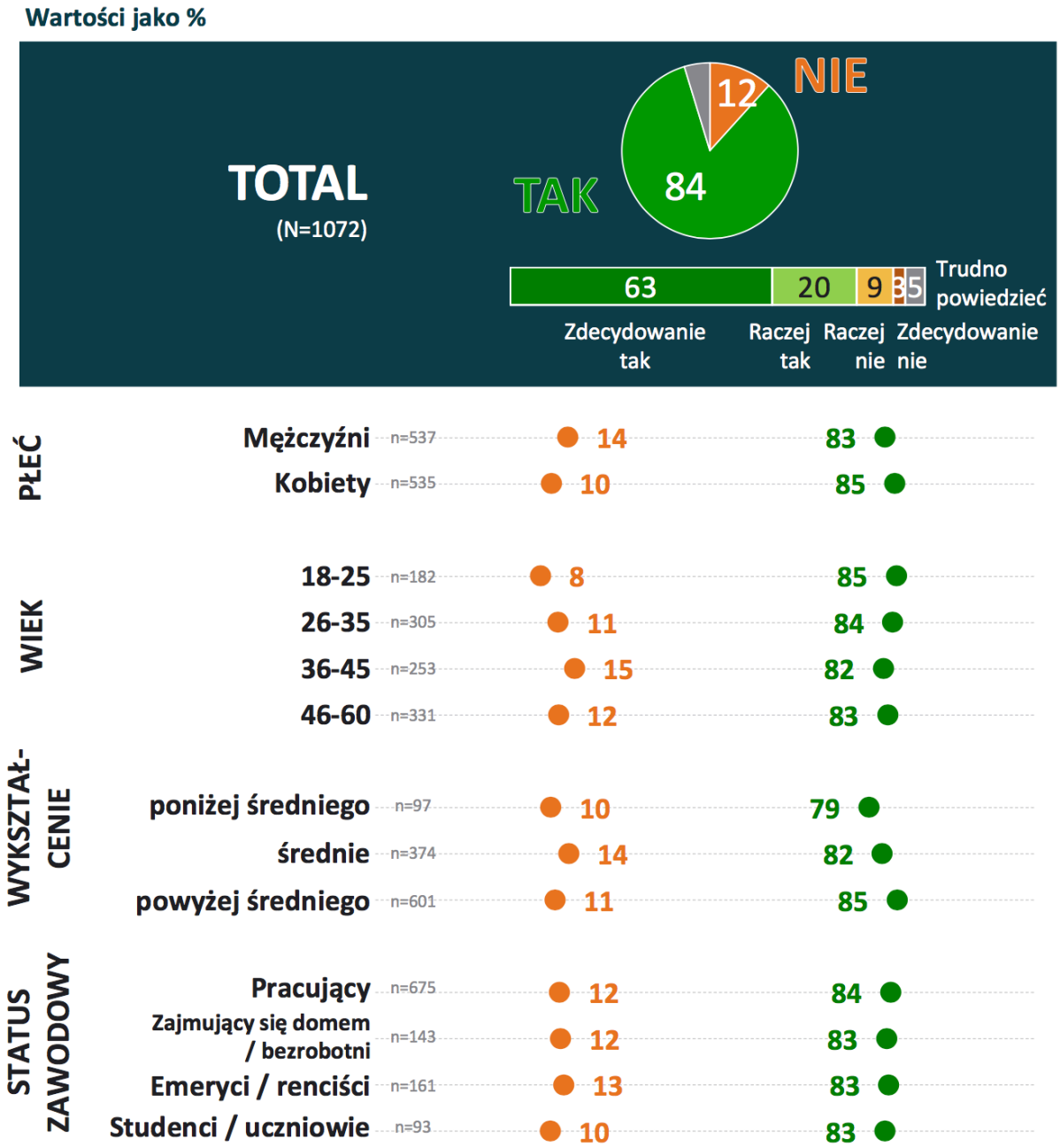


Na pytanie o przyczyny sprzeciwu wobec gromadzenia przez Państwo danych zakupowych respondenci odpowiadali najczęściej, że są one ich prywatną sprawą – słowo „prywatność" pojawiało się w wypowiedziach respondentów najczęściej ze wszystkich wyróżnionych słów kluczowych. Co trzeci sprzeciw uzasadniany był tym, że gromadzenie przez Państwo tych danych kojarzy się z inwigilacją i kontrolą lub stanowi naruszenie wolności osobistych. 11% sprzeciwiających się wskazywało, że nie rozumie po co takie dane miałyby być zbierane i do czego miałyby Państwu służyć.

Pomimo nasilenia w mediach informacji o możliwym wycieku danych z bazy PESEL w czasie realizacji badania, zaledwie 2% respondentów spontanicznie wspominało o obawie o bezpieczeństwo danych.

7.4.6 Czy dostęp do danych o zakupach byłby naruszeniem prywatności?

Czy uważa Pan/Pani, że dostęp instytucji państwowych do danych o wszystkich Pana/Pani zakupach i wydatkach byłby naruszeniem Pana/i prywatności?

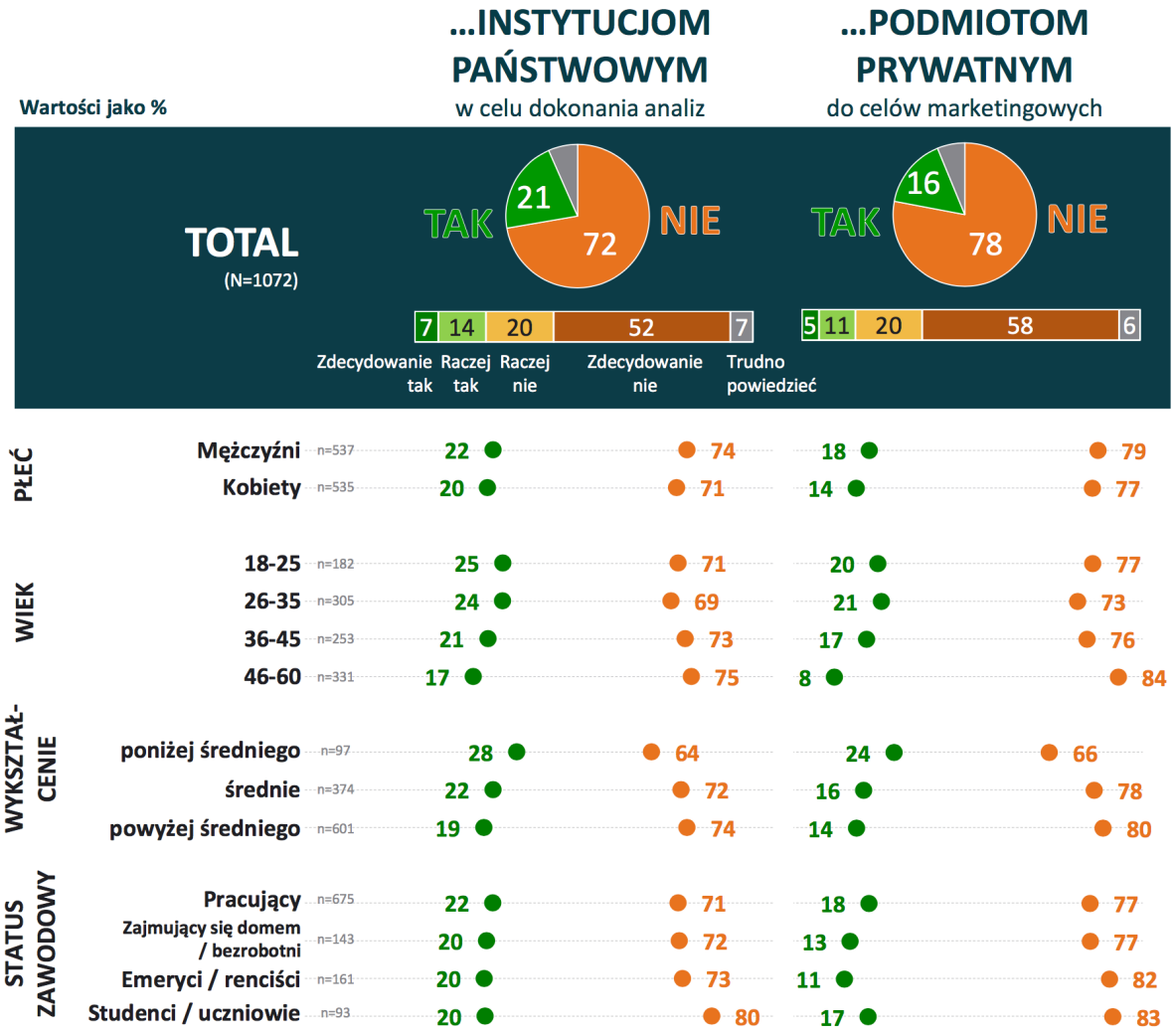


Zdaniem zdecydowanej większości respondentów (84%) dostęp instytucji państwowych do danych o ich zakupach byłby naruszeniem prywatności. Udział odpowiedzi twierdzących jest w tym pytaniu stosunkowo spójny we wszystkich grupach respondentów. Zdecydowanie twierdząco odpowiedziały blisko 2/3 ankietowanych.

7.4.7 Zgoda na udostepnienie informacji o zakupach instytucjom państwowym i podmiotom prywatnym

Czy wyraziłby/wyraziłaby Pan(i) zgodę, by informacje o wszystkich Pana/i zakupach mogły być udostępnianie...

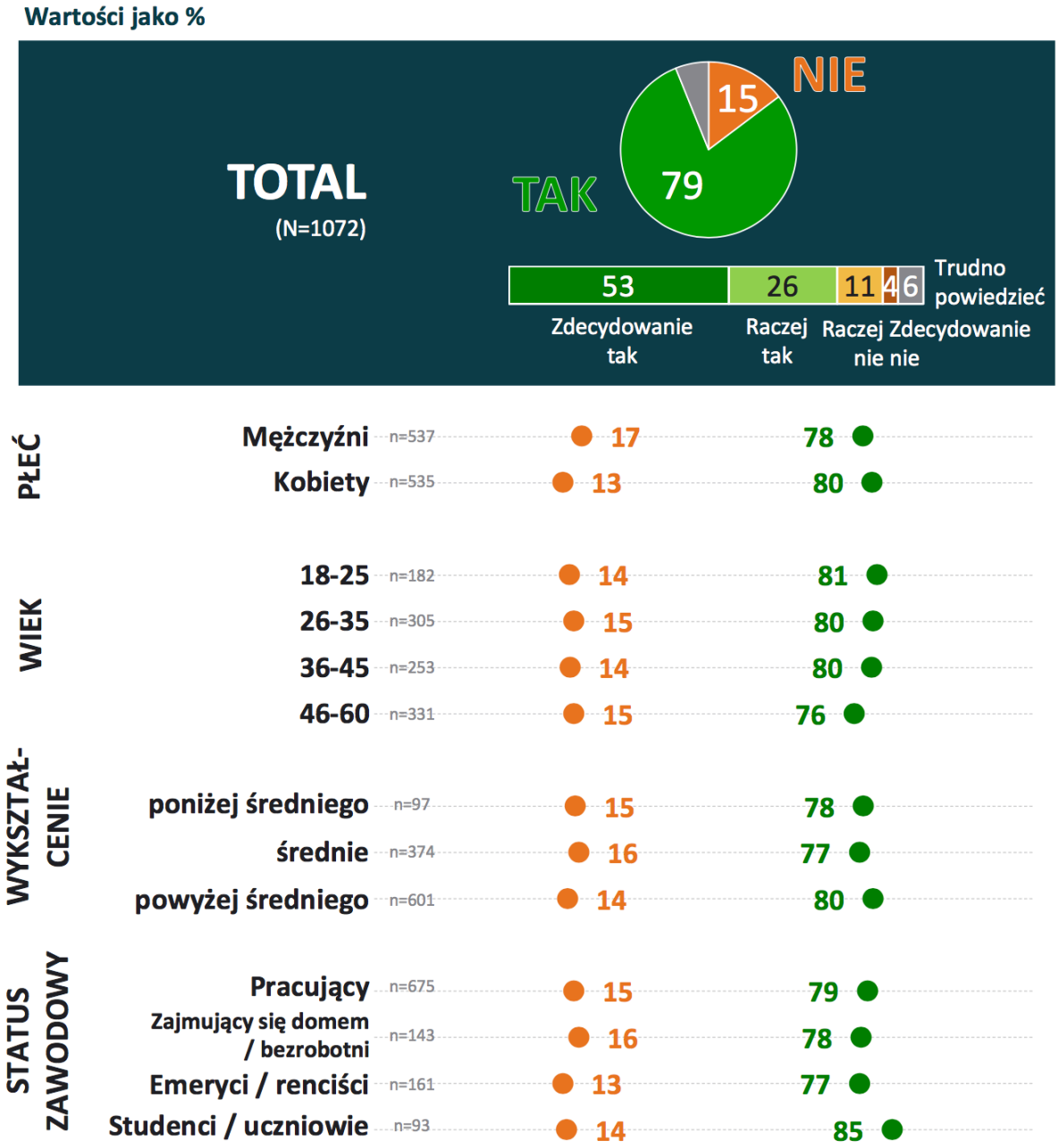
1) *instytucjom państwowym w celu dokonywania analiz?*
2) *podmiotom prywatnym do celów marketingowych?*



72% ankietowanych nie wyraziłoby zgody na udostepnienie danych o swoich zakupach do analiz instytucjom publicznym, a 78% - podmiotom prywatnym do celów marketingowych. W tej kwestii większość badanych wyrażała zdecydowane poglądy – na oba pytania „zdecydowanie nie" odpowiedziała ponad połowa respondentów.

7.4.8 Obawa o bezpieczeństwo danych

Czy obawiał(a)by się Pan/i o bezpieczeństwo danych dotyczących wszystkich Pana/Pani zakupów, jeśli byłyby gromadzone przez państwo?

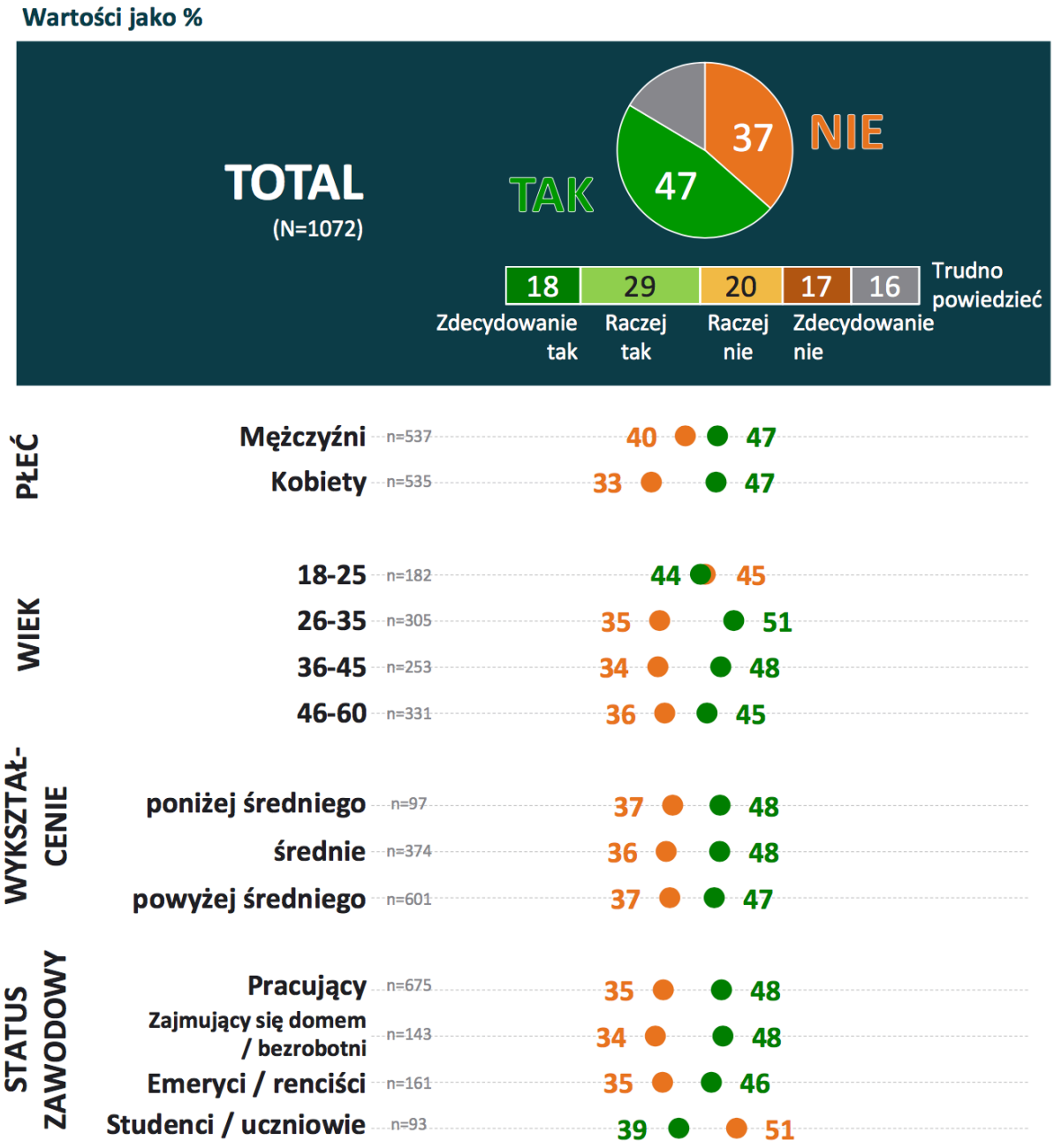


Chociaż respondenci dość rzadko spontanicznie wykazywali obawę o bezpieczeństwo danych zakupowych (gdyby były one gromadzone przez Państwo), to zdecydowana większość potwierdzała tę obawę w pytaniu zamkniętym. Zapytani wprost, czy obawialiby się o swoje dane z e-paragonów, zdecydowana większość (80%) odpowiedziała twierdząco. Nieco większy odsetek obawiających się wycieku danych zaobserwowano wśród respondentów młodszych (do 45 roku zżycia – 80%), szczególnie uczniów / studentów (85%).

Wyraźnie większość, że podczas gdy starsze grupy są nieco bardziej „wyczulone" na kwestie prywatności, to młodsi częściej świadomi są realnych zagrożeń związanych z gromadzeniem ich danych.

7.4.9 Gotowość do samodzielnej analizy własnych danych zakupowych

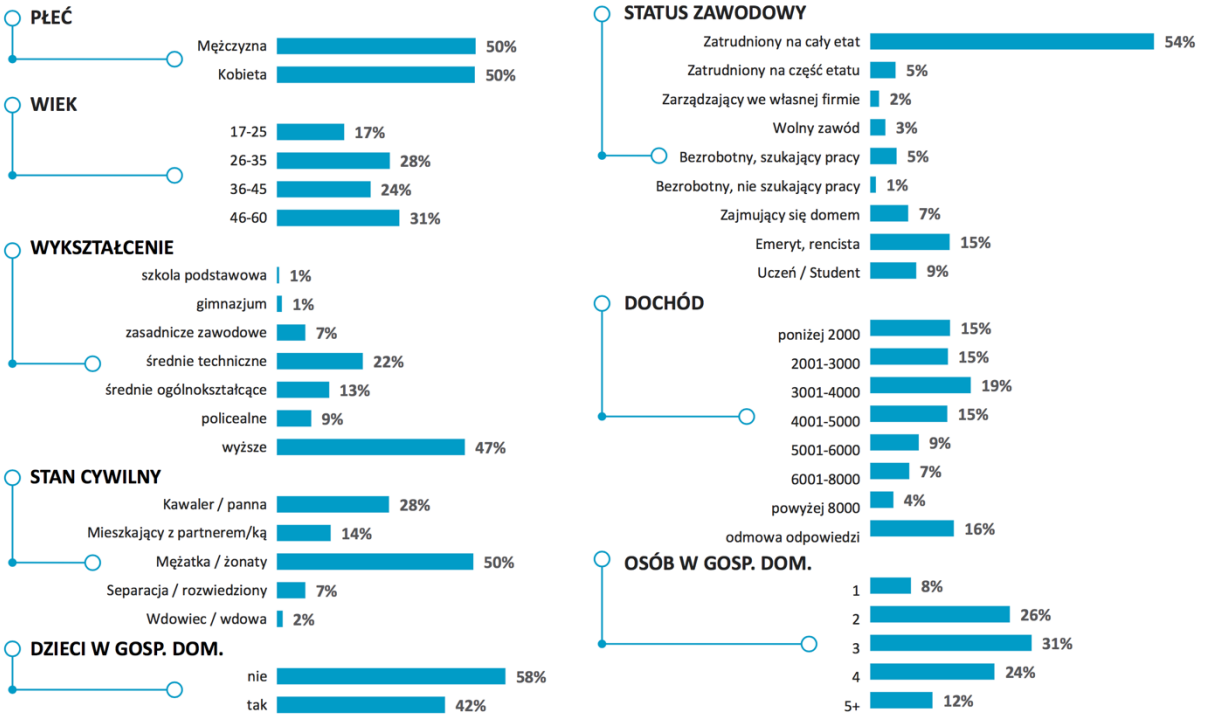
Czy sam(a) dokonywał(a)by Pan(i) analizy zebranych danych o Pana/Pani zakupach, jeśli byłyby one udostępnione Panu(i) w Internecie?



Niecała połowa ankietowanych stwierdziła, że sama analizowałaby swoje dane zakupowe, gdyby były im one udostępnione w Internecie. Prawdopodobnie jednak realny odsetek takich osób byłby dużo niższy (przynajmniej początkowo). W połączeniu z dużym sprzeciwem wobec e-paragonów wynik ten wskazuje na brak entuzjazmu wobec tej idei. Korzyści płynące z tego rozwiązania wydają się nie być wystarczająco atrakcyjne, aby zrekompensować respondentom naruszenie prywatności spowodowane gromadzeniem ich danych zakupowych.

7.4.10 Informacje o respondentach

Badanie zostało przeprowadzone na próbie 1072 Polaków:



7.4.11 Główne wnioski z badań społecznych

- Za wprowadzeniem e-paragonów (wiedząc, że będzie się to wiązało z gromadzeniem przez Państwo danych zakupowych) opowiedziało się 26% respondentów, a przeciw było 62%.
- Całkowite przejście na płatności elektroniczne cieszy się nieco większym poparciem, niż elektroniczne paragony (32% za, 55% przeciw), jednak większość respondentów przeciwna jest także i temu rozwiązaniu.
- Respondentom brakuje uzasadnienia dla idei elektronicznych paragonów: mniej niż połowa ogółu (47%) twierdzi, że samodzielnie analizowałaby swoje dane zakupowe, a nie wyrażający zgody na gromadzenie danych zakupowych przez Państwo często pytają o cel takiego rozwiązania (po co / co to kogo obchodzi?).
- Respondenci młodsi są nieco bardziej skłonni zgodzić się na gromadzenie i udostępnianie ich danych zakupowych, niż starsi. Jednocześnie wśród młodszych częściej pojawiają się obawy o wyciek danych.
- Im wyższe wykształcenie respondentów, tym rzadziej zgadzają się na gromadzenie i udostępnianie swoich danych zakupowych.

7.5 Wyniki badań wśród specjalistów bezpieczeństwa teleinformatycznego

W celu zweryfikowania obaw obywateli, których świadomość w zakresie ochrony prywatności, technologii informatycznych i bezpieczeństwa teleinformatycznego mogła być różna, zadecydowano by przeprowadzić badania sondażowe wśród specjalistów bezpieczeństwa teleinformatycznego, czyli osób posiadających ponadprzeciętną wiedzę na temat funkcjonowania i zabezpieczania systemów informatycznych.

7.5.1 Metodyka badania

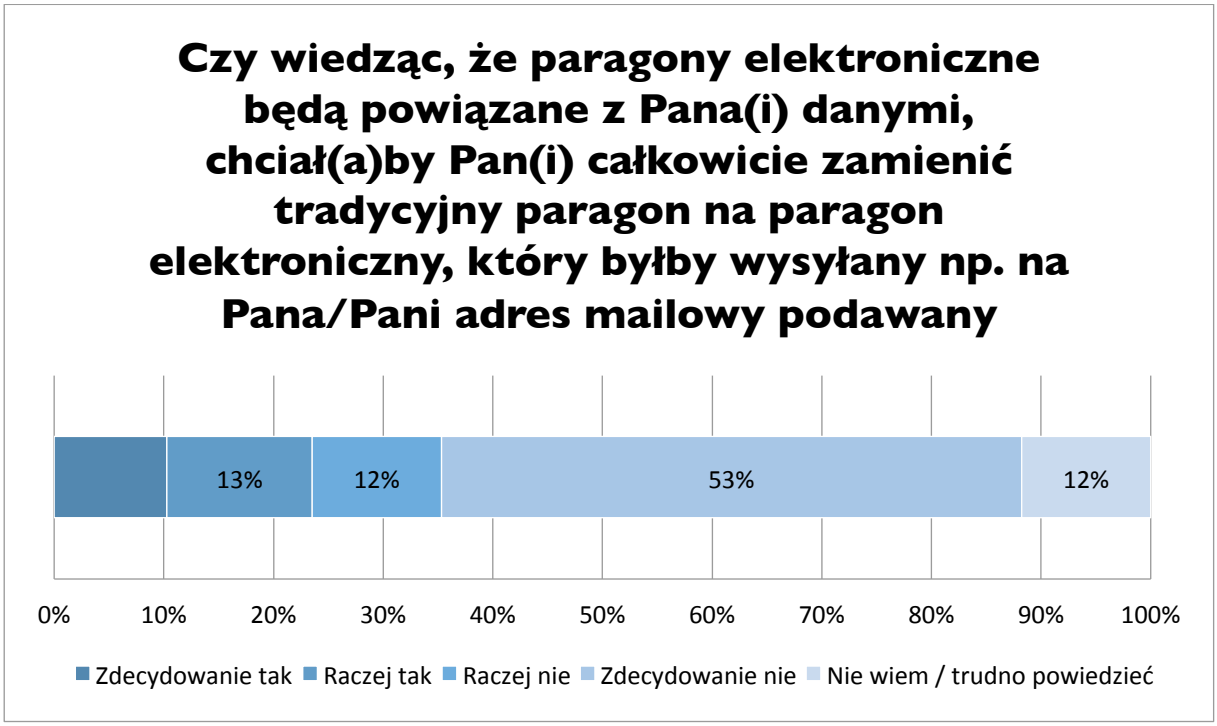
Badanie zrealizowane zostało w trakcie konferencji poświęconej bezpieczeństwu teleinformatycznemu Security Case Ostudy w dniach 14 i 15 września 2016 r. na próbie ok. 60 osób. Uczestnicy po każdej z prelekcji, za pomocą elektronicznego systemu ankietowego odpowiadali na wybrane z badania opisywanego w poprzednim rozdziale pytania.

Zadano 7 pytań zamkniętych z odpowiedziami w skali 1 - 4 (zdecydowanie tak / raczej tak / raczej nie / zdecydowanie nie) oraz kilka pytań profilujących respondentów.

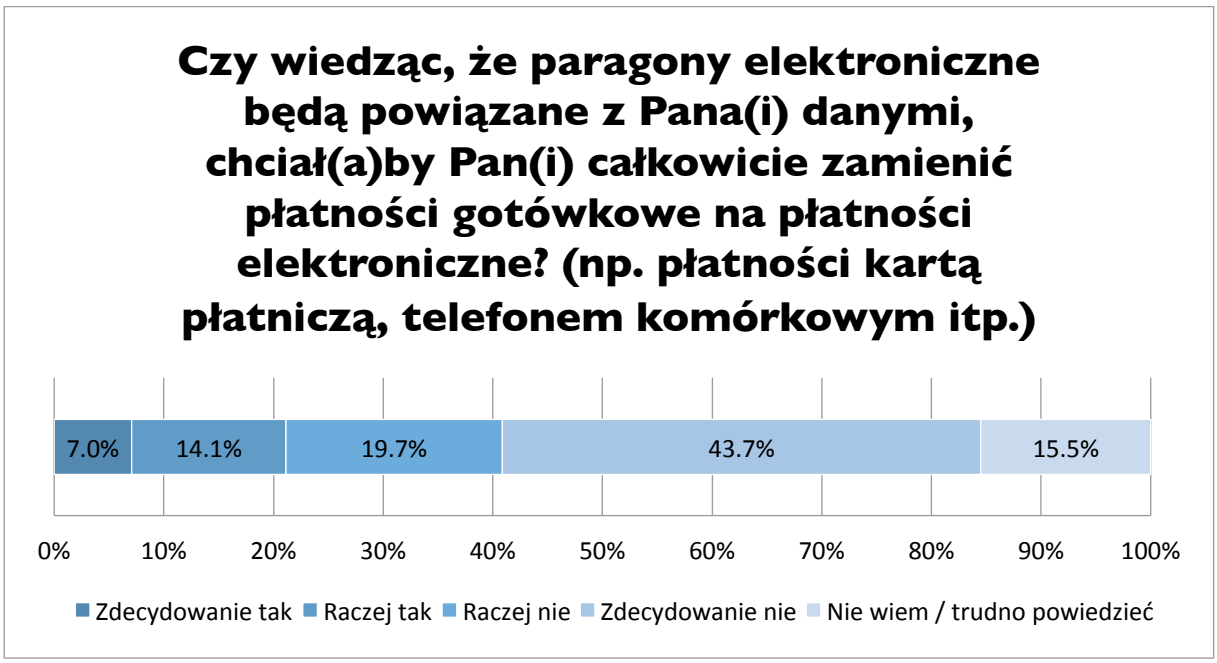
7.5.2 Cel badania

Określenie dominujących wśród specjalistów bezpieczeństwa teleinformatycznego postaw wobec elektronicznych paragonów w kontekście gromadzenia przez Państwo danych zakupowych w powiązaniu z danymi osobowymi.

7.5.3 Poparcie dla przejścia na paragony elektroniczne i transakcje elektroniczne

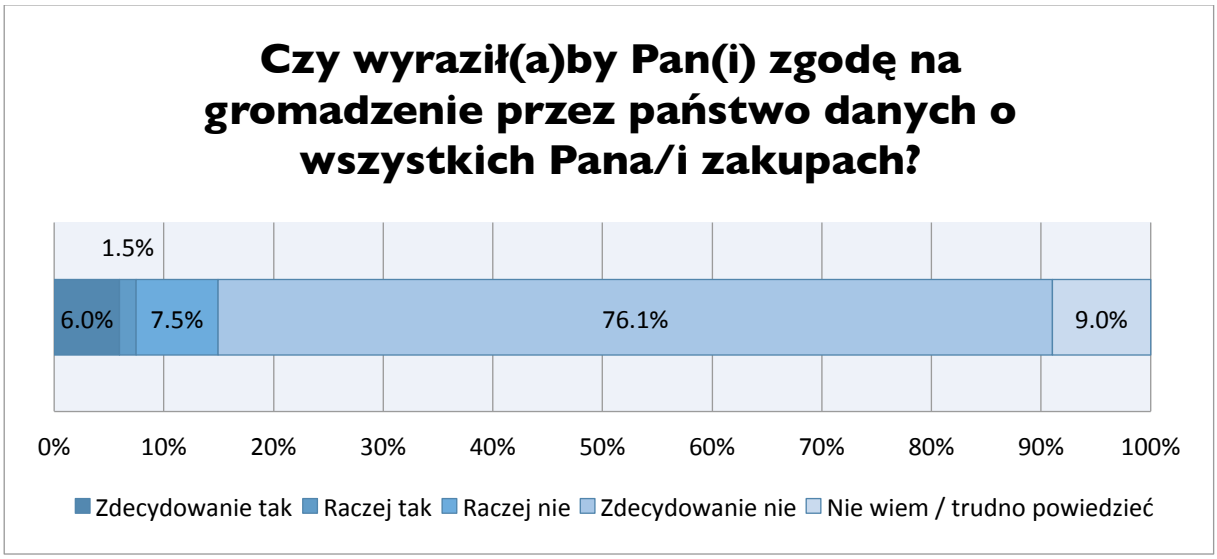


65 % specjalistów jest przeciwnych elektronicznej wersji paragonów. To o 3 % więcej niż w przypadku badania ogólnopolskiego. Za e-paragonami opowiedziało się 23 % respondentów.



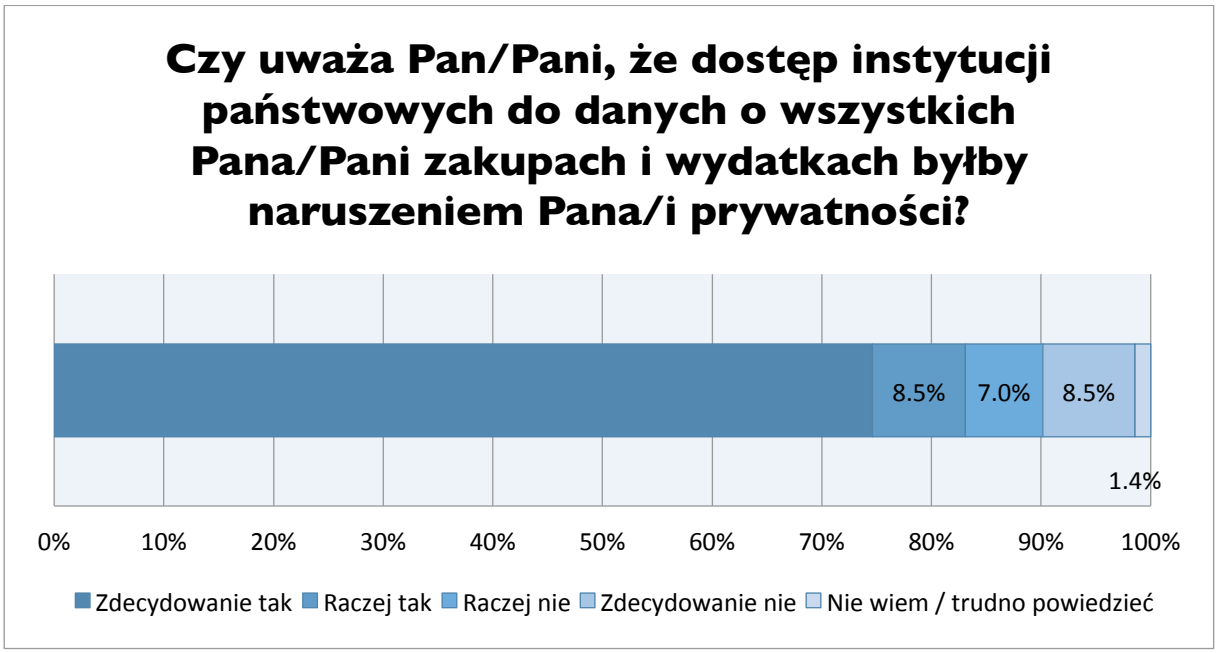
Ponad 63 % przebadanych ekspertów nie chce tej formy płatności elektronicznych. Ponad 8 % więcej niż w przypadku próbki ogólnopolskiej. Zwolennikami płatności elektronicznych było ok 21 % respondentów co w porównaniu do 32 % z badania całego społeczeństwa jest godne uwagi.

7.5.4 Zgoda na gromadzenie danych o zakupach przez Państwo



Duża różnica jest również zauważalna w odpowiedziach na powyższe pytanie. 83,6 % specjalistów nie wyraziłoby zgodny na gromadzenie przez państwo danych o zakupach. W badaniu ogólnopolskim przeciw było 63 % respondentów.

7.5.5 Czy dostęp do danych o zakupach byłby naruszeniem prywatności?

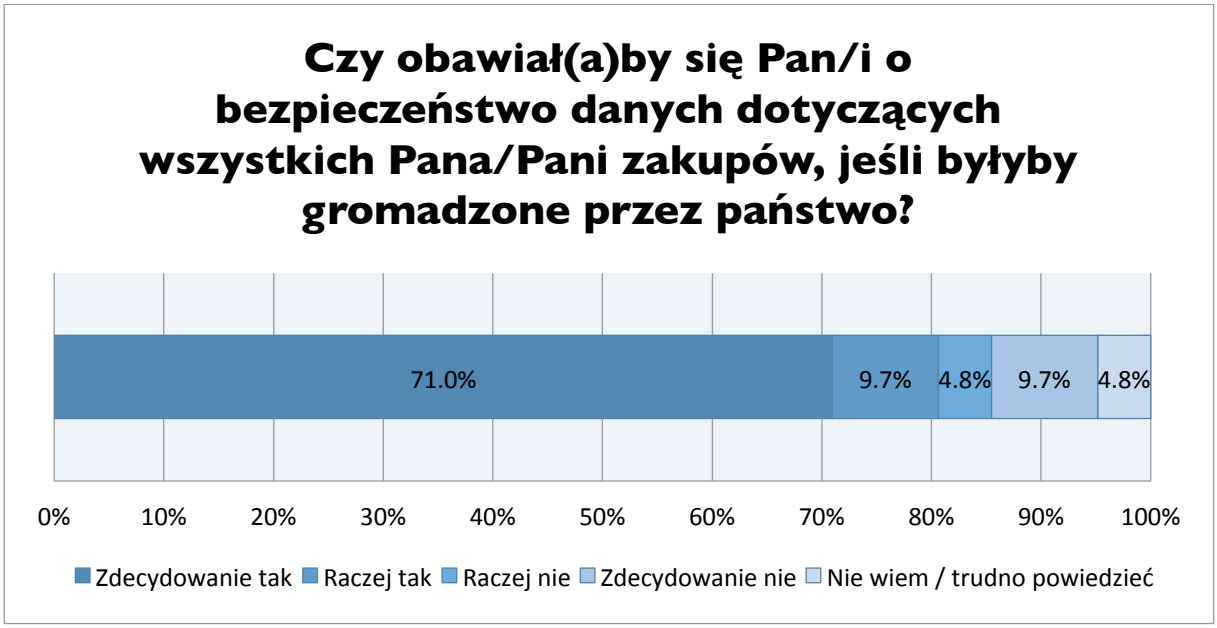


Niemalże identyczne wartości i tym samym pogląd na prywatność wyrazili zarówno specjaliści bezpieczeństwa teleinformatycznego jak i ogólnie społeczeństwo (83,1 % do 84 %). 15,5 % badanych nie uznaje dostępu instytucji państwowych do danych o zakupach za naruszenie prywatności (12 % w poprzednim badaniu).

7.5.6 Zgoda na udostępnienie informacji o zakupach podmiotom prywatnym

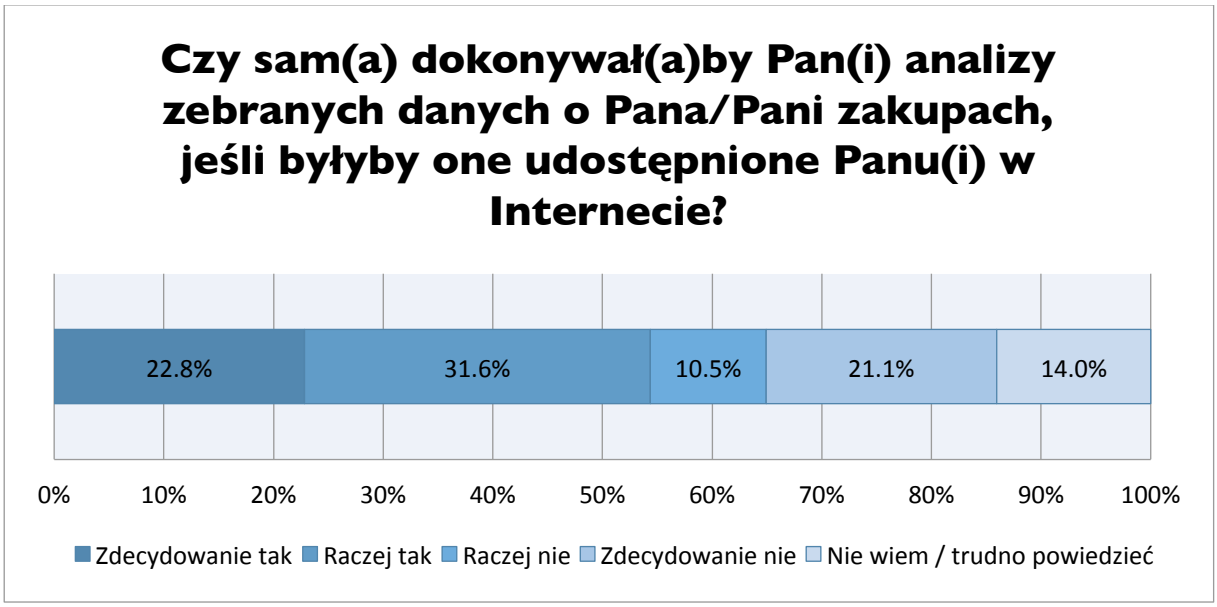
Aż 96% specjalistów nie wyraziłoby zgodny na udostępnienie danych podmiotom prywatnym. Co w porównaniu z badaniem ogólnopolskim (78 %) stanowi znaczną różnicę. Za opowiedziało się 2 % badanych (w badaniu ogólnopolskim 16 %).

7.5.7 Obawa o bezpieczeństwo danych



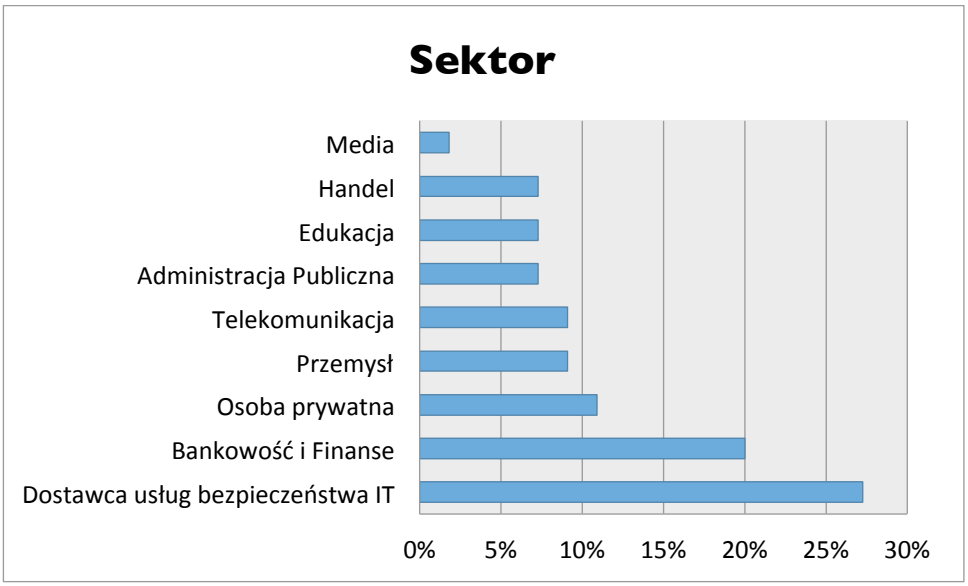
Wyniki porównywalne do badania ogólnopolskiego. Ok. 80 % w obu przypadkach obawia się o bezpieczeństwo danych administrowanych przez administrację. 15 % ufa instytucjom państwowym.

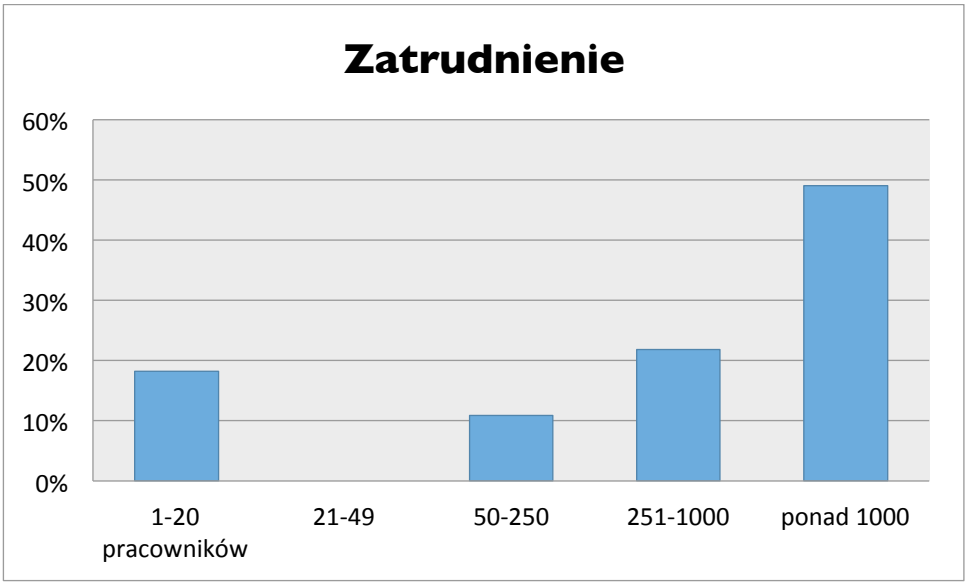
7.5.8 Gotowość do samodzielnej analizy własnych danych zakupowych



Nieco więcej ankietowanych specjalistów deklaruje analizy danych jeśli będą publicznie dostępne (ok 54%l w badaniu ogólnopolskim 47 %). 21 % nie widzi takiej potrzeby.

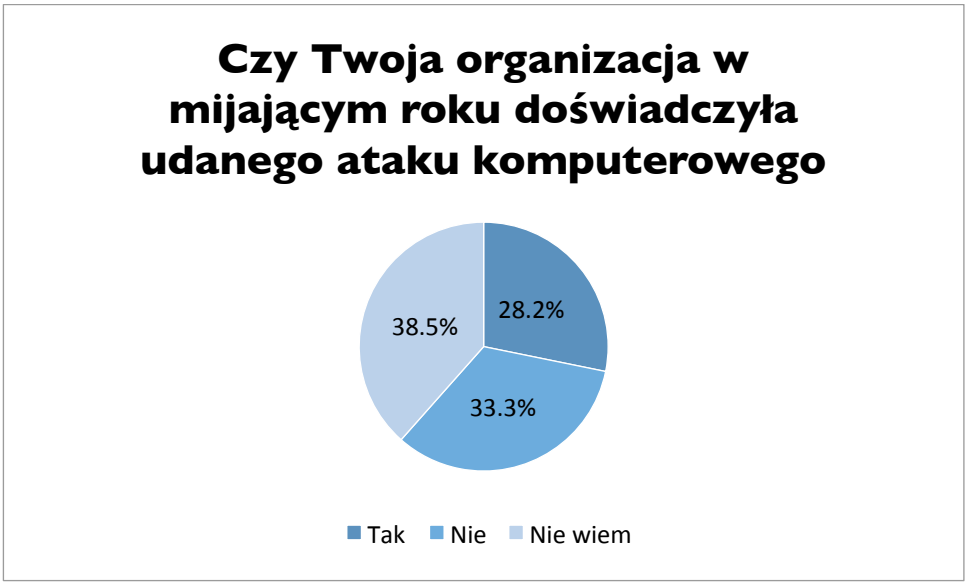
7.5.9 Informacje o respondentach




Zatrudnienie
60%
50%
40%
30%
20%
10%
0%
1-20 pracowników
21-49
50-250
251-1000
ponad 1000


Czy Twoja organizacja posiada wydzielony zespół ds. bezpieczeństwa IT?
12.7%
20.0%
67.3%
Tak
Nie
Nie wiem


Czy Twoja organizacja posiada wydzielony zespół ds. reagowania na incydenty?
16.7%
29.6%
53.7%
Tak
Nie
Nie wiem


Czy Twoja organizacja w mijającym roku doświadczyła udanego ataku komputerowego
28.2%
33.3%
38.5%
Tak
Nie
Nie wiem


Jakiego typu był to atak?
atak na współpracujący podmiot
kradzież pieniędzy z konta
podmiana strony WWW
atak DDoS
włamanie na serwer
wyciek informacji o klientach
wyciek informacji firmowych
kradzież urządzenia
infekcja wirusem
nie dotyczy
0%
10%
20%
30%
40%
50%
60%
70%

8 Wnioski i rekomendacje

8.1 Bezpieczeństwo teleinformatyczne

1. Dane w postaci cyfrowej, scentralizowane w repozytorium, staną się atrakcyjnym celem dla cyberprzestępców. Głównie narażone są gromadzone w ten sposób dane osobowe oraz zbiorcze dane dotyczące zachowań konsumenckich i funkcjonowania rynku.

Rekomendacja: należy możliwie najbardziej ograniczyć wszelkie rozwiązania prowadzące do budowania scentralizowanego repozytorium, w szczególności, kiedy tworzą one nieuzasadnione funkcjonalnością systemu ryzyka dla naruszenia prywatności obywateli.

2. Jednym z głównych celów działań cyberprzestępców jest uzyskiwanie danych kart płatniczych. Tym samym, głównym celem ataków są urządzenia przetwarzające te dane – terminale płatnicze. Ich integracja z urządzeniami rejestrującymi transakcje spowoduje gwałtowny wzrost podatności dla całego systemu, tym bardziej, że system będzie działał w oparciu o sieć Internet. Ze względu na atrakcyjność skutków ataku, możliwe jest systematyczne rozwijanie nowych wektorów ataków, co będzie powodowało wzrost ryzyka i zwiększenie kosztów utrzymania bezpieczeństwa całości systemu.

Rekomendacja: kwestie bezpieczeństwa teleinformatycznego oraz ochrony prywatności powinny odegrać szczególną rolę w ocenie proponowanych zmian w systemie fiskalnym.

3. Ideę przetwarzania danych fiskalnych na dowolnym urządzeniu, dowolnej, niezdefiniowanej przepisami platformie sprzętowej, należy uznać za niebezpieczną dla sprawnego funkcjonowania systemu (powięszkenie powierzchni ataków, wzrost podatności – każda platforma odznacza się innymi; brak jednoznacznych metod audytu czy homologacji).

Rekomendacja: utrzymanie stosowania urządzeń dedykowanych dla funkcji rozliczeń podatkowych.

4. Im system teleinformatyczny jest bardziej złożony i im więcej elementów zawiera, tym jego ochrona jest trudniejsza, a zapewnienie stuprocentowego bezpieczeństwa niewykonalne. Rozwój systemu transakcji fiskalnych w każdym kolejnym etapie zmierza do wzrostu stopnia komplikacji systemu, wzrostu liczby podatności, a tym samym narażenia danych na kompromitację.

Rekomendacja: systemy powinny być projektowane w sposób jak najprostszy, eliminując zbędne interfejsy, urządzenia i podmioty z niego korzystające.

5. Bezpieczeństwo obecnie stosowanego systemu wynika z dwóch aspektów: jego poza sieciowego charakteru (dane rozproszone, przechowywane lokalnie) oraz wysokiej niezawodności urządzeń – kas rejestrujących posiadających dedykowany bezpieczeństwu projekt, urządzenia kryptograficzne i usługi.

Rekomendacja: w systemach koncepcji „e-paragon" nie powinno się rezygnować z zabezpieczeń zarówno po stronie sprzętowej jak i oprogramowania.

6. Nie wszystkie aspekty związane z nowym systemem są prezentowane konsumentom. Przedstawiane propozycje jednostronnie odnoszą się do skutków potencjalnych zmian. Wskazuje się na potencjalne zalety nowego systemu i podejmuje się próby przekonywania konsumentów do przekazywania większej ilości danych niż potrzebne w rozliczeniach fiskalnych podmiotom biorącym udział w proponowanym systemie. Wniosek ten ma szczególną wagę w kontekście

jednoznacznych wyników badań opinii społecznej i grupy eksperckiej, w których widać niewielkie przyzwolenie na wprowadzanie rozwiązań zagrażających prywatności.

Rekomendacja: należy prowadzić proporcjonalną politykę informacyjną, tj. rzeczowo informować o zagrożeniach dotyczących prywatności, w przypadku pozyskiwania i namawiania do przekazywania danych osobowych od konsumentów.

7. Projekt rozporządzenia Ministerstwa Rozwoju w sprawie kryteriów i warunków technicznych, którym muszą odpowiadać kasy rejestrujące z dnia 17.08.2016 r. należy uznać za poprawny pod względem ochrony teleinformatycznej proponowanych rozwiązań. Zastrzeżenia budzą niedookreślone lub nie uzasadnione wymagania w aspekcie interfejsów komunikacyjnych (interfejsu komunikacyjnego, umożliwiającego, co najmniej, współpracę z repozytorium i repozytorium testowym, za pośrednictwem sieci Internet – brak treści załącznika; interfejsu komunikacyjnego umożliwiającego komunikację radiową zgodną ze standardami ISO/IEC 14443 typ A oraz ISO/IEC 14443 typ – brak jasnego uzasadnienia, czy nie jest to pierwsza próba implementacji rozwiązania służącego do przesyłania konsumentom paragonów w formie elektronicznej)

Rekomendacja: należy opracować niezwłocznie brakujące specyfikacje oraz przekazać je do dalszych konsultacji.

8. Budowa centralnego repozytorium danych spowoduje powstanie tzw. single point of failure. Brak jego funkcjonowania w przyszłości, awarie lub kompromitacje danych w nim przetwarzanych będą miały konsekwencje w całym systemie.

Rekomendacja: repozytorium powinno spełniać najwyższe, ogólnie uznawane standardy bezpieczeństwa i przetwarzania danych. Jego uruchomieniu powinna towarzyszyć szczególna staranność dotycząca przeprowadzenia analizy ryzyka.

9. Utrzymanie wysokiej niezawodności metod kryptograficznych w systemie będzie kluczowe.

Rekomendacja: zastosowanie dedykowanych urządzeń i mechanizmów kryptograficznych powinno być standardem dla systemu „e-paragon".

10. Homologacja Głównego Urzędu Miar sprzętu i oprogramowania jest jednym z ważniejszych czynników oddziaływujące na system transakcji fiskalnych.

Rekomendacja: należy utrzymać system wymagający homologacji oraz zapewnić Głównemu Urzędowi Miaro odpowiednie kompetencje osobowe.

8.2 Nastroje i opinie społeczne

1. Społeczeństwo polskie w większości nie chce korzystać z kopii elektronicznej paragonów, ani obrotu bezgotówkowego jeśli miałoby się to wiązać z przekazywaniem dodatkowych danych podmiotom trzecim.

Rekomendacja: systemy dążące do pozyskania danych o klientach należy wdrażać w ograniczonym zakresie. Proces wdrażania powinien zostać wprowadzony zgodnie z mechanizmem pot-in wraz z jasnym poinformowaniem o ryzykach (tak jak na przykład jest to konieczne przy ryzykowanych inwestycjach finansowych).

2. Społeczeństwo uważa, że gromadzenie danych spersonalizowanych jest naruszeniem prywatności obywatela i w zdecydowanej większości nie chce ich przekazywać ani instytucjom państwowym, ani podmiotom prywatnym.

Rekomendacja: prywatność użytkownika powinna być najwyższą wartością wpisywaną we wszelkie dokumenty strategiczne i powinna być poważnie brana pod uwagę przy projektowaniu systemów.

3. Polacy nie ufają poziomowi bezpieczeństwa w instytucjach publicznych.

Rekomendacja: należy zadbać o odpowiedni poziom bezpieczeństwa systemów publicznych, dobór kadry i jej kompetencje.

4. Grupa specjalistów ds. bezpieczeństwa teleinformatycznego jest jeszcze bardziej skrajna w swoich poglądach od ogółu społeczeństwa.

Rekomendacja: specjaliści bezpieczeństwa teleinformatycznego powinni mieć jeden z wiodących głosów przy konsultacji założeń i projektowaniu systemów teleinformatycznych.

5. Nie ulega wątpliwości, że pomimo negatywnego nastawienia społeczeństwa, poprzez prowadzenie działań lobbujących obrót bezgotówkowy, a tym samym coraz większy stopień przekazywania danych o konsumentach podmiotom takim jak instytucje finansowe, aspekt bezpieczeństwa teleinformatycznego i ochrony prywatności będzie marginalizowany w przyszłości.

Rekomendacja: Należy niezwłocznie rozpocząć działania uświadamiające o zagrożeniach teleinformatycznych związanych z transakcjami elektronicznymi i wartości danych, w tym osobowych w cyberprzestrzeni. Należy dołożyć wszelkich starań, zarówno przez organizacje rządowe jak i pozarządowe, by konsumenci byli w pełni świadomi jakie dane i komu przekazują korzystając z szeroko pojętych e-usług.

FUNDACJA BEZPIECZNA CYBERPRZESTRZEŃ
Pozarządowa organizacja non-profit, której celem, jest działanie na rzecz bezpieczeństwa cyberprzestrzeni, w tym na rzecz poprawy bezpieczeństwa w sieci Internet. Osiągnięcie tych celów fundacja realizuje poprzez działalność w trzech głównych obszarach: UŚWIADAMIANIA o zagrożeniach teleinformatycznych, REAGOWANIA na przypadki naruszania bezpieczeństwa w cyberprzestrzeni, prowadzenia DZIAŁALNOŚCI BADAWCZOROZWOJOWEJ w dziedzinie bezpieczeństwa teleinformatycznego.

FUNDACJA BEZPIECZNA CYBERPRZESTRZEŃ
ul. Tytoniowa 20, 04-228 Warszawa
tel: +48 22 112 0 800
e-mail: kontakt@cybsecurity.org

www.cybsecurity.org

FUNDACJA
bezpieczna
cyberprzestrzeń