Cyberdefence 24

28.05.2020

NIEBEZPIECZNE KASY WIRTUALNE. MINISTERSTWO FINANSÓW NARAZI PRZEDSIĘBIORCÓW NA CYBERATAKI?

Ministerstwo Finansów w niejasnych okolicznościach wprowadza rozszczelnienie systemu kas fiskalnych poprzez skierowanie branż z wysokim prawdopodobieństwem oszustw podatkowych do systemu, który jeszcze nie istnieje i zawiódł w wielu krajach na świecie. W tle pojawia się konieczność wymiany kas przez przedsiębiorców.

Ustawa z dnia 15 marca 2019 r. o zmianie ustawy o podatku od towarów i usług oraz ustawy - Prawo o miarach wprowadziła rewolucyjne zmiany w systemie kas fiskalnych. Ustawa weszła w życie z dniem 1 maja 2019 r. Nowelizacja ta wprowadziła zupełnie nowy typ kas rejestrujących, tzw. kasy fiskalne online.

W odróżnieniu od kas pierwszej generacji, kasy online automatycznie przekazują do Centralnego Repozytorium Kas informacje o transakcjach wraz ze szczegółami pozwalającymi na ustalenie wysokości podstawy opodatkowania, kwot podatku należnego, stawki, rodzaju towaru/usługi, a także czasu i miejsca instalacji kasy. W zakresie poprawy szczelności systemu podatkowego prowadzenie kas online jest odpowiednikiem pliku JPK w ewidencji faktur. Dla użytkowników kas nie rodzi dodatkowych obowiązków, ponieważ komunikacja z bazą danych jest automatyczna. Kasy te zachowują najwyższy poziom bezpieczeństwa nawet będąc poza zasięgiem internetu. Wszystkie informacje archiwizowane są też lokalnie w urządzeniu i zabezpieczone także w sposób fizyczny – poprzez brak dostępu do modułu fiskalnego.

Przejście na nowy system wprowadzane jest stopniowo, wg. grup przedsiębiorców wskazanych przez MF w rozporządzeniach. Grupy te zostały wybrane na podstawie m.in. oceny, które branże wymagają uszczelnienia systemu rejestracji obrotu.

Pierwsza grupa przedsiębiorców, którzy mają obowiązek stosowania kas online od stycznia 2020 r. to stacje benzynowe i mechanicy. Dalszy plan z 2019 roku obejmował grupy: (2) Lipiec 2020 r - gastronomia, usługi krótkotrwałego zakwaterowania, sprzedaż węgla. (3) Styczeń 2021 r. - branża budowlana, usługi fryzjerskie, kosmetyczne, lekarzy i dentyści, kluby fitness i usługi prawnicze. Obecnie grupa z lipca została przeniesiona na styczeń w związku z epidemią koronawirusa.

Generacja trzecia – „lex Uber”

2 kwietnia 2019 rząd przyjął nowelizację ustawy o transporcie drogowym, potocznie nazywaną „Lex Uber”, która po przyjęciu przez sejm obowiązuje od 1-01-2020. Projekt oprócz uporządkowania zasad przewozu osób wprowadził możliwość stosowania aplikacji mobilnej jako alternatywy wobec obecnie stosowanego taksometru i kasy fiskalnej. Oznacza to, że projekt wprowadził trzecią generację kas fiskalnych – w formie oprogramowania instalowanego na dowolnym urządzeniu użytkownika. Aplikacje

takie powszechnie nazywane są „kasami wirtualnymi”.

Przed wejściem w życie przepisów konieczne było przygotowanie przez MF rozporządzenia wykonawczego dotyczącego kas fiskalnych i taksometrów oraz notyfikacja ich w Komisji Europejskiej. Dlatego wprowadzony został okres przejściowy do 31 marca. Ponieważ MF zwlekał z publikacją rozporządzenia pozwalającego traktować aplikacje jako legalne narzędzie rozliczania się klienta z kierowcą okres przejściowy został wydłużony do 1 października.

Dotychczas wszystko wskazywało, że kasy wirtualne mają być dla administracji skarbowej technologiczną nowinką, która używana będzie punktowo w przewozie osób i na podstawie tych doświadczeń może być wprowadzona szeroko w kolejnych latach.

Kasy wirtualne przedstawiane są jako kolejna generacja i ułatwienie dla przedsiębiorców. Na podstawie rozporządzenia technicznego MF widać, że pod względem bezpieczeństwa i zachowania szczelności systemu fiskalnego są krokiem wstecz wobec kas online. „Aplikacja kasowa” może być przygotowane przez dowolnego dostawcę, zainstalowana na dowolnym telefonie lub tablecie i nie musi być połączona z certyfikowanym, sprzętowym rejestratorem transakcji. Oznacza to, że np. w „Google Play” obok aplikacji fiskalnej będzie aplikacja do „cofania licznika” transakcji. Jest to całkiem możliwy scenariusz wyłudzenia, ponieważ kasa może działać także offline i łączyć się z siecią np. raz dziennie. Kreatywność twórców obejść systemu może być nieograniczona, a odpowiedzialność za dostarczenie narzędzi zerowa. Scenariusz ten potwierdzają przypadki np. z Austrii czy Chorwacji.

11 maja 2020 Ministerstwo Finansów zaproponowało, aby w pilotażu kas wirtualnych wzięło udział nie tylko 60 tys. kierowców przewozu osób, ale także 75 tys. przedsiębiorców z branż, które wcześniej zakwalifikowane zostały jako priorytetowe do uszczelnienia systemu podatkowego. Przedsiębiorczy zostaną postawieni przez wyborem, czy mają przejść na kasy online czy na kasę wirtualną, czyli wykupić abonament i używać kasy jako jednej z aplikacji na smartfonie wirtualną, czyli wykupić abonament i używać kasy jako jednej z aplikacji na smartfonie. Doprowadzi to do arbitrażu systemowego, gdzie przedsiębiorcy zainteresowani unikaniem ewidencji sprzedaży przejdą na powstający dopiero system kas wirtualnych i będą stanowili nieuczciwą konkurencję dla przedsiębiorców działających zgodnie z prawem, często prowadzących sprzedaż tuż obok.

Ryzyko cyberataków

O konieczności zadbania o odpowiednie standardy cyberbezpieczeństw apelował też pełnomocnik rządu ds. cyberbezpieczeństwa. Pisał, że realizacja funkcji fiskalnych wykorzystująca warstwę oprogramowania (aplikacji) wymaga przeprowadzenia pełnej analizy ryzyk dla integralności i dostępności danych. W jego opinii zastosowanie aplikacji wprowadza nowe wektory ataków, które dotychczas ograniczane były przez mechanizmy zabezpieczające, stosowane w warstwie sprzętowej kas fiskalnych. Analiza ta powinna wskazać minimalne zabezpieczenia organizacyjne i techniczne, których celem ma być ograniczenie ataków i nadużyć z wykorzystaniem nowego środowiska kas fiskalnych bazującego na oprogramowaniu i urządzeniu mobilnym.

Pełnomocnik zwracał również uwagę, że w projekcie rozporządzenia brak jest odwołań do metod oraz kryteriów badania i certyfikacji integralności oprogramowania wykorzystywanego do realizacji funkcji kas fiskalnych uruchamianego w środowisku urządzenia mobilnego, co może umożliwić przeprowadzenie ataku np. na ścieżkę aktualizacji oprogramowania dla raportów fiskalnych.

Przedmiotowy projekt nie wskazuje także minimalnych wymagań bezpieczeństwa dla urządzeń mobilnych. Konieczne jest odesłanie do minimalnej specyfikacji technicznej (m.in. wersja systemu operacyjnego, mechanizmy kryptograficzne i ich bezpieczna implementacja). Nie określono także wymagań dla zarządzania bezpieczeństwem środowiska aplikacji (np. z poziomu systemu

centralnego) oraz jej separacji od innych aplikacji uruchamianych na urządzeniu, które mogą umożliwiać zakłócenie funkcjonowania aplikacji fiskalnej.”

Obawy o bezpieczeństwo kas wirtualnych ma również KIGEiT. Eksperci organizacji zauważają, że rozwiązania opisane w projekcie nie są prawidłową implementacją technologii „document-chain” ponieważ nie zawierają rozproszonej bazy danych działającej w trybie online. Taka implementacja nie zabezpiecza przed usuwaniem z urządzenia ostatnich paragonów przed ich wysłaniem do repozytorium w przypadku gdy kasa wirtualna jest odłączona od Internetu. Istnieje sposób aby takie paragony usunąć bez śladu i po podłączeniu do Internetu kontynuować sprzedaż, tak jakby tamtych paragonów w ogóle nie było – czytam w opinii KIGEiTu. Eksperci zwracają również uwagę na fakt, że rozporządzenie w obecnym kształcie nie zawiera mechanizmów pozwalających zablokować sprzedaż w przypadku braku połączenia kasy wirtualnej z Internetem o ile tylko klucz współdzielony (pobrany przez kasę z serwera) zachowuje ważność w rozpatrywanym okresie. W granicznym przypadku kasa może działać bez połączenia z Internetem nawet przez 72 godziny (jeżeli odłączenie od Internetu nastąpi zaraz po pobraniu trzech kluczy współdzielonych, z których każdy jest ważny przez 24 godziny).

W rozporządzeniu nie są określone żadne szczegółowe wymagania czy obostrzenia dla nośnika kasy np. tzw. hardeningu systemu jak też kryteria uznania, kiedy środowisko jest „odpowiednie” dla funkcjonowania kasy – ostrzegają eksperci KIGEiTu Nie określono jakie są możliwości aktualizacji środowiska, np. systemu operacyjnego, co jest normą przy systemach tzw. konsumenckich z systemami operacyjnymi Windows/IOS/Android. Nie są określone ograniczenia współużytkowania innych aplikacji instalowanych na tym samym urządzeniu.

Nie określono w jaki sposób poszczególne wymagania bezpieczeństwa mają być zrealizowane, aby osiągnąć zamierzony skutek szczelności, oraz w jaki sposób ma być to zweryfikowane na etapie badań certyfikacyjnych, oraz – co wydaje się najważniejsze – jak ma być zapewnione egzekwowanie bezpiecznych warunków użytkowania Kasy Wirtualnej u podatnika.

Dodatkowo wydaje się, że MF bagatelizuje lub nie widzi zagrożenia, które leży gdzie indziej. Nie ma potrzeby klonowania kasy fiskalnej. Znacznie niebezpieczniejsze z punktu widzenia rozszczelnienia systemu jest korzystanie na jednym urządzeniu z dwóch identycznie wyglądających dla kasjera i nabywcy programów: autentycznego, certyfikowanego i zafiskalizowanego oprogramowania kasy wirtualnej oraz oprogramowania stworzonego specjalnie w celu unikania rejestrowania sprzedaży przypominającego do złudzenia w zakresie interfejsu użytkownika i emitowanych wydruków autentyczną kasę wirtualną. Przełączając te programy nieuczciwy podatnik otwiera sobie wielkie pole do nadużyć – ostrzega KIGEiT.

Wnioski

Kasy fiskalne w formie oprogramowania miały być wąsko stosowanym rozwiązaniem wprowadzonym jako techniczne rozporządzenie do ustawy „lex Uber”. Z niewyjaśnionych przyczyn Ministerstwo Finansów od początku dążyło do szerokiego wprowadzenia na rynek wirtualnych kas wirtualnych. Bez fazy testów i przy nieprzygotowanym do tego systemie centralnym. De facto oznaczałoby to rozszczelnienie systemu fiskalizacji sprzedaży poprzez „testowanie” nowej technologii na 145 tys. przedsiębiorstw, z których cześć należy do grupy wysokiego ryzyka. Braki w przygotowaniu odpowiednich zabezpieczeń narażają przedsiębiorców, którzy zdecydują się na wdrożenie takiego rozwiązania.