Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji

Warszawa, dn. 26.05.2020 r.
KIGEiT/1478/05/2020

Oświadczenie Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji na publikacje medialne Ministerstwa Finansów

Wczoraj ukazał się wywiad Pełnomocnika Ministra Finansów ds. Informatyki, Pana Przemysława Kocha[1]. Według najlepszej wiedzy naszych ekspertów szereg informacji przekazanych w wywiadzie nie ma pokrycia w faktach i może wprowadzać czytelnika w błąd.

Poniżej odnosimy się do poszczególnych wypowiedzi przedstawiciela Ministerstwa Finansów:

„Zastosowaliśmy nowatorskie rozwiązanie na polskim rynku, tzw. document-chain, które wywodzi się z koncepcji block-chain. Daje ono pewność, że nikt nie manipulował przy paragonach, nie usunął ich z kasy, bądź nie dorzucił do nich tzw. pustych paragonów. Każdy kolejny paragon i jego identyfikator będzie zależał od wszystkich wcześniej wystawionych, ich wartości, itp. Jakakolwiek manipulacja przy paragonach spowoduje przerwanie łańcucha dokumentów, co zostanie natychmiast wykryte po stronie fiskusa w oparciu o algorytmy sztucznej inteligencji - zapewnił Koch."

Powyższe stwierdzenie nie jest prawdziwe. Rozwiązania opisane w projekcie nie są w rzeczywistości 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.

„Jednocześnie, jak dodał, kasa wirtualna będzie przekazywać wszystkie wygenerowane dokumenty fiskalne w interwałach co jedną minutę. To - zdaniem Kocha – także ogranicza możliwość dokonania niezauważonej manipulacji. W sytuacji awarii, czy braku dostępu do internetu będzie można prowadzić sprzedaż w trybie off-line, ale nie dłużej niż 15 minut. Po tym czasie kasa straci możliwość rejestrowania sprzedaży, aż do czasu ponownego zalogowania do sieci."

W notyfikowanym przez UE projekcie nie ma mowy o wspomnianych przez p. Kocha 15 minutach. 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).

Z przepisów notyfikowanego rozporządzenia:
W przypadku nieprzesłania danych kasa:
- *umożliwia dalszą ewidencję, sygnalizując w sposób czytelny dla użytkownika przekroczenie zadanego terminu zgodnego z harmonogramem przesyłania danych;*

[1] https://www.bankier.pl/wiadomosc/MF-wirtualne-kasy-fiskalne-beda-bezpieczne-7890593.html

ul. Stępińska 22/30, 00-739 Warszawa, tel.: +48 22 8510309, 8406522, e-mail: kigeit@kigeit.org.pl, https://kigeit.org.pl;
NIP 5260029121 Konto: BNP PARIBAS O/Warszawa nr: 52 1600 1374 0003 0052 2279 1001

- *podejmuje automatyczne próby kolejnego przesyłania danych nie rzadziej niż co 2 godziny pracy kasy.*

Kasa pobiera klucze współdzielone co najmniej raz na dobę.

- *Kasa nie może prowadzić ewidencji bez ważnego klucza współdzielonego na dany dzień.*

Częstotliwość łączenia się kasy z repozytorium jest konfigurowalna i rzeczywiście to łączenie może następować co minutę. Zaznaczyć należy, że taki tryb pracy przewidziany był jako specjalny, stosowany w stosunku do podatników znajdujących się w obszarze zainteresowania. Taki tryb pracy stawia zupełnie inne wymagania wydajności dla centralnego repozytorium. Ale to nadal jednak nie będzie to system online i dlatego nadal będzie możliwość skorzystania z narzędzi pozwalających oszustom w czasie przerw między kolejnymi połączeniami z Internetem na usuwanie danych sprzedaży. Każda techniczna zmiana w projekcie wymagałaby ponownej notyfikacji rozporządzenia.

„Jeżeli wykryjemy nieprawidłowości, możemy centralnie sterować każdą kasą wirtualną, możemy też skrócić interwały czasowe raportowania, albo czas, w którym kasa może pracować w trybie off-line. Możemy wysłać komendę do kasy z żądaniem ponownego przekazania dowolnych dokumentów z kasy w celu kontroli, czy weryfikacji - dodał."

Nie jest prawdą, że Ministerstwo Finansów ma możliwość bezpośredniego sterowania kasami wirtualnymi. To kasa musi połączyć się z repozytorium, pobrać przeznaczone dla niej zadania i dopiero później je zrealizować. Centralne sterowanie kasą ograniczone jest jedynie do wymuszenia powtórnego odesłania danych oraz do zmiany częstotliwości przesyłania danych i pobierania kolejnych zadań. W notyfikowanym rozporządzeniu nie ma możliwości ustawienia czasu pracy kasy wirtualnej w trybie off-line.

„W ramach certyfikacji GUM będzie potwierdzał, że kasa działa zgodnie z wymaganiami określonymi w rozporządzeniu, w szczególności, czy jest odpowiednio zabezpieczona przed możliwością przypadkowego skasowania lub manipulacji danych z kasy. Oprogramowanie, które nie będzie spełniać określonych wymogów nie uzyska certyfikatu i nie będzie mogło być używane."

GUM będzie badał jedynie oprogramowanie kas wirtualnych. A zatem pozostawiono lukę, dzięki której oszuści będą mogli ingerować w działanie kasy wirtualnej poprzez ingerencję w system operacyjnym lub sprzęt na którym działa kasa wirtualna.

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. Nie określono jakie są możliwości aktualizacji środowiska, np. systemu operacyjnego, co jest normą przy systemach tzw. konsumenckich z systemami operacyjnymi Widnows/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.

„Koch odniósł się także do twierdzenia, że kasę będzie można „sklonować" i prowadzić „na boku" sprzedaż poprzez kasę, która nie będzie podłączona do systemu ministerstwa.

Przewidzieliśmy mechanizmy zabezpieczające przed +sklonowaniem+ kasy. Kasa będzie fiskalizowana na określonym sprzęcie; telefonie, tablecie, czy komputerze, będzie przekazywać do

MF +odcisk palca+ tego sprzętu. W trakcie życia urządzenia będziemy sprawdzać, czy ów +odcisk+ nie zmienia się, ktoś nim nie manipuluje, bądź nie zmienia urządzenia, na którym program jest zainstalowany - dodał Koch."

W rozmowie P. Koch powołuje się na zabezpieczenia („odcisk palca"), które nie występują w projekcie rozporządzenia. 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.

„Nie ma też możliwości, aby kasa migrowała między urządzeniami. Na przykład w razie zniszczenia urządzenia, kasa musi być dezaktywowana, trzeba będzie zarejestrować nową kasę i ponownie przejść proces jej fiskalizacji - poinformował."

To w żaden sposób nie zabezpiecza przed opisanymi powyżej oszustwami – autentyczna kasa nie musi migrować pomiędzy urządzeniami – na każdym z tych urządzeń można zainstalować autentyczną kasę wirtualną i oprogramowanie ją udające. W przypadku aplikacji jest to bezproblemowe podczas gdy w przypadku kas sprzętowych niewykonalne.

„Według niego kolejnym rozwiązaniem zwiększającym bezpieczeństwo kas wirtualnych są tzw. tokeny. Kasa, która przejdzie proces fiskalizacji, będzie raz na trzy dni pobierać z MF „tokeny" w postaci ciągu znaków wyliczonych w oparciu o funkcje kryptograficzne. Będą one dawać kasie możliwość prowadzenia sprzedaży.

Każdego dnia kasa będzie musiała użyć innego tokena otrzymanego z MF. Jeżeli nasz system analityczny wykryje nieprawidłowości, możliwość pobrania kolejnych tokenów może zostać zablokowana, a Krajowa Administracja Skarbowa może wszcząć kontrolę u danego przedsiębiorcy lub w miejscu, gdzie taka kasa działa - powiedział."

Nie bardzo wiadomo, czemu miałoby służyć manipulowanie przy tokenach, skoro są prostsze sposoby oszukiwania na kasach wirtualnych.

„Zgodnie z zapowiedziami Kocha, w drugiej połowie roku resort finansów chce udostępnić aplikację mobilną pozwalającą na weryfikację paragonów wystawianych przez kasy wirtualne. "Każdy paragon, który będzie wystawiany przez kasę wirtualną będzie opatrywany kodem QR. Aplikacja MF pozwoli na weryfikację każdego paragonu bez względu, czy będzie wystawiony elektronicznie, czy papierowo. Klient będzie mógł zeskanować kod QR i sprawdzić, czy paragon został przesłany fiskusowi - wytłumaczył pełnomocnik."

Takie narzędzie zakłada pełną współpracę nabywców, którzy masowo biorąc udział w takiej loterii wyłapują oszustów. Założono wobec tego, że:

- Większość społeczeństwa posiada urządzenia, na których można zainstalować i uruchomić taką aplikację.
- Osoby, które zainstalowały taką aplikację przy okazji każdego zakupu będą chciały zeskanować kod QR z paragonu.
- W przypadku kłopotów z zeskanowaniem, będą ponawiały próby aż do skutku.
- W przypadku niepowodzenia zezwolą na wysłanie przez aplikację informacji o tym fakcie do MF.

Jeżeli powyższe warunki nie będą spełnione, to oszuści będą mogli opatrywać podrobione paragony nieczytelnymi kodami QR albo w przypadku sprzedaży takich samych towarów/ usług w kody QR uzyskane z autentycznych paragonów co będzie bardzo trudne do wykrycia.

Prezes Zarządu

Stefan Kamiński

Signature Not Verified

Dokument podpisany przez Stefan Kamiński; KIGEiT
Data: 2020.05.26 15:39:45 CEST