Bezpieczeństwo systemu fiskalnego

Jednym z modeli rozpatrywanym obecnie przez rząd w tematyce kas on-line jest system oparty o „wirtualną kasę fiskalną” *(tzw. model chorwacki / słoweński / czeski).*

Przeniesienie funkcjonalności specjalizowanych urządzeń rejestrujących (*kas fiskalnych – w Polsce pracuje około 2 mln takich urządzeń) posiadających szereg mechanizmów bezpieczeństwa, do aplikacji instalowanej na dowolnym, niezaufanym urządzeniu (takim będzie komputer, tablet, smartphone lub inne urządzenie z rynku konsumenckiego z uniwersalnym systemem operacyjnym*) oznacza zignorowanie wszelkich zagrożeń występujących w świecie cyfrowym. Rozwiązanie to zamiast zwiększać lub co najmniej utrzymywać obecny poziom bezpieczeństwa w miejscu realizacji transakcji, wprowadza szereg zagrożeń i w efekcie może prowadzić do rozszczelnienia systemu fiskalnego w Polsce.

Aktualne raporty z zakresu bezpieczeństwa w sieciach i systemach teleinformatycznych (*np.: Raport roczny z działalności CERT Polska „Krajobraz bezpieczeństwa polskiego internetu 2015”*), statystyki dotyczące rozprzestrzeniania „złośliwego oprogramowania” (*wirusy, rootkity, trojany, ransomware itd.)*, i wzmagające się działania organizacji przestępczych w sektorze internetowym prowadzą do zupełnie odmiennej polityki – przechodzenia z rozwiązań programowych na rozwiązania sprzętowe tam gdzie tylko jest to możliwe.

Na niezaufanym urządzeniu - nie posiadającym kontroli ingerencji do wnętrza, bez dedykowanych mechanizmów ochronnych, bez dedykowanego systemu operacyjnego (OS) możliwe jest zainstalowanie dowolnych dodatkowych aplikacji mogących przypadkowo lub celowo zakłócać pracę e-kasy, prowadząc do fałszowania rzeczywistej sprzedaży.

Certyfikacja samej aplikacji jest na pewno właściwa (*jeśli chcemy mieć pewność, że sama aplikacja działa poprawnie i nie realizuje funkcji szkodliwych*), nie jest jednak wystarczająca z powodu braku kontroli nad środowiskiem, w którym działa.

Niekontrolowane środowisko może praktycznie w dowolny sposób wpływać na działanie aplikacji, w szczególności modyfikując dane na każdym etapie ich przetwarzania. Wystarczy dostęp szkodliwego oprogramowania (*zainstalowanego lokalnie na niezaufanym urządzeniu lub kontrolującego to urządzenie zdalnie*) do zasobów systemowych urządzenia (*np. pamięci, interfejsy wejścia-wyjścia*), z których korzysta również aplikacja e-kasa, aby możliwe było dowolne modyfikowanie danych zanim zostaną one zabezpieczone i przesłane do serwerów agregujących dane fiskalne.

Jako jedyny właściwy sposób zapewnienia zabezpieczenia i „uszczelnienia” systemów teleinformatycznych, obecnie są postrzegane rozwiązania sprzętowe, z racji wbudowanych mechanizmów bezpieczeństwa oraz separacji od możliwych zagrożeń poprzez unikalność swojej budowy (*są to rozwiązania dedykowane do realizacji wyłącznie zaplanowanych funkcjonalności*).

Tylko połączenie bezpiecznych dedykowanych rozwiązań sprzętowych z kontrolowanym oprogramowaniem tworzy kompletne środowisko zapewniające właściwy poziom bezpieczeństwa. Przykłady systemów „kompletnych”:

- obsługa płatności w punktach sprzedaży.(np: organizacje płatnicze Visa i MasterCard);
- gry, zakłady losowe typu „Lotto”;
- terminale obsługi użytkownika stosowane np. przez firmy kurierskie;
- przekazywanie danych wrażliwych w instytucjach Państwowych (policja, wojsko itp.).