Ważna rekomendacja

Krzysztof Wojdyło

17 listopada 2015 r. Komisja Nadzoru Finansowego wydała bardzo ważną rekomendację dotyczącą bezpieczeństwa transakcji płatniczych wykonywanych w internecie. Powinna ona zostać wnikliwie przeanalizowana przez każdy podmiot, który jest zaangażowany w realizację płatności elektronicznych.

Problem bezpieczeństwa w cyberprzestrzeni, w tym bezpieczeństwa rozliczeń dokonywanych on-line, to niewątpliwie jedno z najważniejszych obecnie wyzwań zarówno dla informatyków, jak i prawników. Liczba spraw dotyczących różnych form cyberprzestępstw rośnie w ostatnim czasie lawinowo. Tradycyjne instrumenty prawne, w szczególności rozwiązania ustawowe, są tworzone w bardzo wolnym tempie i nie nadążają za dynamicznie zmieniającym się otoczeniem. W takich okolicznościach ranga „miękkich" instrumentów prawnych, takich jak omawiana rekomendacja, znacząco rośnie.

Rekomendacja KNF jest w przeważającej mierze powieleniem rekomendacji wydanych wcześniej przez Europejskie Forum ds. Bezpieczeństwa Płatności Detalicznych oraz Europejski Urząd Nadzoru Bankowego. Reguluje przede wszystkim zagadnienia związane z procesem identyfikacji i uwierzytelniania klienta, monitorowania transakcji oraz ochrony wrażliwych danych płatniczych.

Jedna z kluczowych rekomendacji dotyczy stosowania tzw. silnego uwierzytelniania przy autoryzacji płatności. Silne uwierzytelnienie polega na zastosowaniu przynajmniej dwóch różnych kategorii instrumentów uwierzytelniających określonych w rekomendacji. W przypadku przelewów stosowanie silnego uwierzytelnienia powinno być zasadą, od której rekomendacja przewiduje jednak pewne wyjątki. Również wydawcy kart muszą zapewnić możliwość silnego uwierzytelniania płatności kartowych.

Inna ciekawa rekomendacja odnosi się do popularnej praktyki wykorzystywania przy otwieraniu rachunków przelewu z innego rachunku jako metody weryfikacji podmiotu otwierającego rachunek. Nadzór dopuszcza taką praktykę jedynie w bardzo ograniczonym zakresie. Wykorzystanie tej metody będzie możliwe jedynie w sytuacji, w której rachunek otwarty z wykorzystaniem takiej metody nie będzie mógł być wykorzystany do otwarcia w taki sposób kolejnego rachunku. Wydaje się jednak, że nadal będzie możliwe wykorzystywanie przelewów w celu weryfikacji tożsamości na potrzeby innych usług finansowych niż otwieranie rachunków (np. w związku z udzielaniem pożyczek).

Istotne praktyczne znaczenie będzie miała również zapewne treść rekomendacji dotyczącej monitorowania transakcji. Podaje ona przykłady konkretnych rozwiązań, które powinny być stosowane przez dostawców usług płatniczych w celu wykrywania oszustw (np. w zakresie geolokalizacji adresów IP czy wykrywania oznak infekcji sesji). Rekomendacja ta stanie się zapewne swoistym punktem odniesienia przy ocenie staranności działania banków w zakresie wykrywania oszustw. To z kolei może mieć praktyczne znaczenie przy ewentualnym dochodzeniu od banków roszczeń w związku z coraz częstszymi cyberprzestępstwami.

Warto również zwrócić uwagę na zakres zastosowania rekomendacji. Jest ona adresowana do banków, krajowych instytucji płatniczych, krajowych instytucji pieniądza elektronicznego i spółdzielczych kas oszczędnościowo-kredytowych. Oznacza to, że, przynajmniej formalnie, adresatami rekomendacji nie są instytucje kredytowe lub instytucje płatnicze spoza Polski prowadzące jednak działalność na terytorium Polski. Warto również wskazać, że rekomendacja nie ma zastosowania do płatności mobilnych innych niż realizowane przy użyciu przeglądarki internetowej.