**„Farbowanie” to nie wszystko. Jak skutecznie zabezpieczyć bankomat?**

**Warszawa, 13 października 2021 r.**

**Kilkanaście dni temu opublikowano nowelizację rozporządzenia, które nakłada na banki i operatorów bankomatów obowiązek instalowania systemów uszkadzających banknoty w razie napadu na bankomat lub innych nieuprawnionych działań. Fizyczne zabezpieczenie czy naznaczenie gotówki to tylko jeden z aspektów ochrony urządzeń przed przestępcami.**

W myśl nowych przepisów, bankomaty w Polsce, które nie mają zapewnionej 24-godzinnej fizycznej ochrony będą musiały być wyposażone w inteligentne systemy neutralizacji banknotów (IBNS, z ang. Intelligent Banknote Neutralisation Systems). Systemy te uaktywniają się w razie napadu lub kradzieży pieniędzy z bankomatu i zabarwiają banknoty - zazwyczaj na czerwono, fioletowo lub zielone. Zaplamione banknoty są sukcesywnie usuwane z obiegu gotówkowego przez odpowiednie organy i instytucje państwowe.

Według resortu spraw wewnętrznych, zastosowanie IBNS w funkcjonujących w Polsce bankomatach ma ograniczyć liczbę napadów na bankomaty. Działania przestępców polegające na wysadzaniu czy uszkadzaniu urządzeń są w końcu cały czas realnym problemem. Jak wynika z raportu Związku Banków Polskich, tylko w III kwartale tego roku doszło do 32 napadów na bankomaty. Dla porównania, w pierwszym półroczu 2020 roku miało miejsce co najmniej 70 napadów, a w całym 2019 było ich 165. Niestety, regularnie w mediach pojawiają się kolejne doniesienia o próbach obrabowania bankomatów przez mniej lub bardziej profesjonalnych złodziei.

– Można dyskutować z kształtem nowych przepisów, na przykład w zakresie procentowego uszkadzania banknotów z wykorzystaniem systemów IBNS, ale trudno dyskutować z tym, że każdy bankomat należy zabezpieczyć w maksymalny sposób. Dywagacje na temat odpowiedniego kształtu regulacji będą z pewnością jeszcze się toczyć, ale już teraz warto skupić się na sednie problemu, czyli zapobieganiu przestępstwom – zauważa **Tomasz Rokita, członek zarządu Diebold Nixdrof w Polsce**.

Krajobraz zagrożeń związanych z bezpieczeństwem bankomatów i gotówki wciąż ewoluuje. Ataki i metody stosowane przez przestępców są bardzo zróżnicowane i mogą być niezwykle złożone. Dlatego też należy stale śledzić i badać rozponane zagrożenia, aby lepiej zrozumieć i dostosować wykorzystywane rozwiązania do przeciwdziałania działalności przestępczej. Bezpieczeństwo bankomatów należy analizować w trzech głównych aspektach: bezpieczeństwa cybernetycznego, zabezpieczenia danych i bezpieczeństwa fizycznego.

– Od ponad 160 lat, Diebold Nixdorf chroni gotówkę, dane i aktywa. Rozumiemy, że kontekst jest kluczowy dla bezpieczeństwa, dlatego rozwijamy inteligentne, dopasowane do potrzeb różnych organizacji rozwiązania bezpieczeństwa, które zmniejszają ryzyko i równoważą potrzeby biznesowe z oczekiwaniami klientów w zakresie ochrony prywatności – mówi **Tomasz Rokita**.

**Bezpieczeństwo fizyczne**

Większość ataków fizycznych polega na użyciu materiałów wybuchowych lub taranów, które całkowicie lub częściowo niszczą bankomat czyniąc go bezużytecznym. Przestępcy mogą uzyskać w ten sposób dostęp do znajdującej się w nim gotówki. Tego typu ataki mogą być niezwykle kosztowne, ponieważ banki muszą nie tylko wymienić zniszczony bankomat, ale także uporać się z dodatkowymi szkodami, które mogły powstać w jego otoczeniu.

Rozwiązania bezpieczeństwa z tego zakresu obejmują m. in. inteligentne czujniki mogące wykryć, kiedy złośliwe urządzenia zostaną umieszczone w szczelinie gotówkowej czy kartowej, stalowe obudowy i sejfy w odpowiedniej klasie bezpieczeństwa bardziej odporne na tego typu ataki np. Gasex, system ActivGuard, który wykrywa i inteligentnie raportuje informacje z 12 różnych czujników czy wspomniane wcześniej systemy do neutralizacji banknotów, zgodne z nowymi wymogami prawnymi.

**Cyberbezpieczeństwo**

Cyberataki mają na celu uzyskanie dostępu do gotówki, danych konsumentów lub obu tych elementów. Przestępcy na całym świecie przeprowadzali ataki typu "jackpot", w ramach, których wprowadzali do systemów bankomatowych złośliwe oprogramowanie lub manipulowali oprogramowaniem bankomatów w celu wykonywania nielegalnych transakcji poprzez ataki typu "blackbox”.

Dzięki odpowiedniemu oprogramowaniu, można w czasie rzeczywistym identyfikować, raportować i analizować nietypowe zdarzenia, jak na przykład nadmierna liczba wypłat gotówki przy użyciu tej samej karty, co może oznaczać atak typu „jackpot”. Zastosowanie właściwych rozwiązań cyberbezpieczeństwa pozwala również na centralne zarządzanie wszystkimi zdarzeniami związanymi z bankomatami i alertami bezpieczeństwa, a także zdalny roll-out zaktualizowanych polityk bezpieczeństwa.

**Zabezpieczenie danych**

Skimming jest największym zagrożeniem w kategorii zabezpieczenia danych klientów. Ataki skimmingowe na bankomaty mogą kosztować bank setki tysięcy złotych, nie licząc szkód dla marki i utraty zaufania konsumentów do bankomatów i samej instytucji finansowej. Technologia skimmingu staje się coraz bardziej zaawansowana, ułatwiając przestępcom kradzież danych właścicieli kart za pomocą elektroniki przymocowanej gdzieś w bankomacie - najczęściej na czytniku kart, z dodatkowymi kamerami skierowanymi na PIN pad. Przestępcy są obecnie w stanie stworzyć skimmer, który jest tak cienki jak kartka papieru.

Bankomaty z rodziny DN Series oferują szeroki zestaw rozwiązań obejmujący modułowe, skalowalne opcje zapewniające bezpieczeństwo danych i ochronę przed skimmingiem. Wśród nich jest system rozpoznający nawet najcieńsze skimmery, który zapobiega wprowadzeniu cienkiego jak brzytwa wewnętrznego skimmera dzięki algorytmowi, który rozpoznaje, kiedy urządzenie zostało umieszczone wewnątrz czytnika kart na zbyt długo.

Więcej informacji na temat rozwiązań DN Series dla banków można znaleźć na stronie [www.dieboldnixdorf.com](https://www.dieboldnixdorf.com/en-us/banking/portfolio/systems/dn-series).