

BEZPIECZNE PŁATNOŚCI

Dynamiczny rozwój technologii cyfrowych nieodwracalnie zmienia sposób, w jaki konsumenci i firmy dokonują transakcji finansowych. Nowoczesne formy płatności – od mobilnych portfeli przez płatności zbliżeniowe po rozwiązania biometryczne i kryptowaluty – zyskują na popularności, oferując wygodę, szybkość i coraz wyższy poziom bezpieczeństwa. Jednak wraz z tym postępem pojawiają się również nowe wyzwania: rosnące ryzyko cyberataków, potrzeba zgodności z regulacjami oraz konieczność budowania zaufania użytkowników.

Celem niniejszego raportu jest przedstawienie aktualnych trendów w obszarze płatności cyfrowych, identyfikacja najważniejszych zagrożeń oraz analiza kierunków, w których zmierza rynek. Raport pokazuje, jak sektor finansowy, regulatorzy i dostawcy technologii wspólnie pracują nad zapewnieniem, by przyszłość płatności była nie tylko innowacyjna, ale przede wszystkim bezpieczna.



Jak chronić środowisko płatności

Jak podaje raport Narodowego Banku Polskiego, w III kw. 2024 r. w Polsce przeprowadzono 2,7 mld transakcji kartami płatniczymi, a na koniec września ub.r. funkcjonowało ponad 1,3 mln terminali POS (point-of-sale) do przyjmowania takich płatności. Ich liczba systematycznie rośnie, a transakcje bezgotówkowe stały się standardową i preferowaną formą płatności, ale – jak wszystkie inne cyfrowe udogodnienia – są narażone na cyberzagrożenia. Kluczem do zwiększenia ich bezpieczeństwa jest odpowiednia ochrona środowisk urządzeń POS.

ROBERT DĄBROWSKI

szeft zespołu inżynierów w polskim oddziale Fortinet

Systemy POS występują w różnych formach, dobieranych zależnie od potrzeb przedsiębiorstwa związanych z obsługą transakcji sprzedażowych – od prostych terminali płatniczych po zaawansowane systemy łączące funkcje sprzedażowe i analityczne. Często jest to zwykły terminal do płacenia kartą, ale w przypadku sklepów detalicznych może być to komputer połączony z ekranem dotykowym, bazą danych i kasą fiskalną. Niezależnie od liczby połączonych urządzeń i ich typu jeden aspekt ich funkcjonowania się nie zmienia – podczas płatności kartą aplikacje POS przetwarzają przypisane do niej informacje i dane osobiste właściciela. Dlatego środowiska point-of-sale stanowią wrażliwy punkt, a z tego powodu wystawione są

na cyberzagrożenia. Przechowywane w nich dane mogą być wykorzystane do kradzieży pieniędzy, a także popełnienia po-

ważnych oszustw dotyczących kradzieży tożsamości.

Typowy atak na POS rozpoczyna się od uzyskania przez



przestępcę dostępu do systemu ofiary przy wykorzystaniu luki w zabezpieczeniach albo użyciu metod socjotechnicznych. Następnie haker instaluje złośliwe oprogramowanie zaprojektowane do kradzieży danych kart kredytowych z systemów POS i terminali płatniczych. Jeśli jego praca powiedzie się, zebrane informacje przesyłane są do zewnętrznego repozytorium. Co więcej, atak wymierzony w jedno urządzenie może w szybkim tempie rozprzestrzenić się na inne w obrębie tej samej sieci, jeśli taka była intencja cyberprzestępców.

SKUTECZNE METODY OCHRONY SYSTEMÓW POS

Istnieje wiele sposobów, aby zapewnić dobrą ochronę sys-

temowi POS. Wybierając najlepsze praktyki i dostosowane do swoich potrzeb narzędzia, firmy mogą zmaksymalizować swoje szanse na odparcie cyberataków.

Aby skutecznie zabezpieczyć systemy POS, właściciele firm oraz pracujący dla nich specjaliści ds. cyberbezpieczeństwa powinni wprowadzić w życie kilka podstawowych praktyk, stosowanych także w innych cyfrowych rozwiązaniach. Szyfrowanie end-to-end zabezpiecza dane transakcyjne od chwili ich wprowadzenia do systemu POS aż do momentu dotarcia do banku lub procesora płatności. Uniemożliwia to wyciek informacji nawet w przypadku naruszenia bezpieczeństwa urządzenia POS. Kolejną bardzo ważną metodą ochrony jest uwierzytelnianie dwuskładnikowe, które polega na użyciu dodatkowego sposobu weryfikacji użytkownika podczas logowania. Zazwyczaj jest to dodatkowy kod wysyłany przez SMS, podawany w aplikacji lub wyświetlany na fizycznym przedmiocie (tokenie), a więc w taki sposób, że dostęp do takiego kodu ma tylko upoważniona osoba. W niektórych urządzeniach POS istnieje także możliwość stworzenia białej listy (white list) zawierającej wyłącznie te aplikacje, które mogą pracować na danym urządzeniu (uruchomienie wszystkich pozostałych zostanie zablokowane).

Jedną z taktyk umożliwiających zwiększenie poziomu bezpieczeństwa jest korzystanie z oprogramowania POS zainstalowanego na tabletach iPad

firmy Apple. Ich system operacyjny (iOS) charakteryzuje się wieloma ograniczeniami związanymi z równoległą obsługą wielu aplikacji w danym momencie, co może skutecznie utrudnić uruchomienie działającego w tle, równocześnie z systemem POS, szkodliwego oprogramowania do wykradania informacji.

**BARDZO WAŻNĄ
METODĄ OCHRONY JEST
UWIERZYTELNIANIE
DWUSKŁADNIKOWE,
KTÓRE POLEGA NA
UŻYCIU DODATKOWEGO
SPOSOBU WERYFIKACJI
UŻYTKOWNIKA PODCZAS
LOGOWANIA.**

Należy jednak pamiętać, że podstawą i pierwszą linią dobrej ochrony powinna być odpowiednio wyszkolona kadra pracownicza. Pracownicy, którzy nie mają odpowiedniej świadomości zagrożeń, są podatni na sztuczki socjotechniczne albo pominięcie wytycznych bezpieczeństwa. Mogą więc potencjalnie ułatwiać przeprowadzenie udanego ataku na system POS, przy którym złodziej nie będzie musiał stosować żadnych wyrafinowanych technik, aby zapewnić sobie sukces. Pracownicy mogą też ukraść lub zgubić urządzenia z zainstalowanym



oprogramowaniem point-of-sale, co otwiera możliwość uzyskania dostępu do systemu każdemu, kto je znajdzie.

Scenariusz, w którym to osoba pracująca w danej placówce jest odpowiedzialna bezpośrednio za atak, jest rzadko spotykany, ale możliwy. Dlatego sprzedawcy powinni blokować swoje aplikacje pod koniec każdego dnia oraz w każdej chwili, gdy urządzenie POS nie jest używane. Dodatkowym środkiem ostrożności jest ciągłe monitorowanie zachodzących procesów w systemie. Implementując te praktyki, przedsiębiorca zmniejsza ryzyko wynikające z błędu lub sabotażu pracownika.

POLSKI WYNALEZEK ODPOWIEDZIA NA ZAGROŻENIA

Odpowiedzialność za ochronę punktu sprzedaży stoi przede wszystkim po stronie użytkującego go przedsiębiorstwa. Są jednak sposoby na zwiększenie swojego poziomu bezpieczeństwa przez konsumentów. Niektóre metody płatności są bezpieczniejsze, a jedną z nich jest BLIK.

Transakcje z zastosowaniem tej metody nie wymagają udostępniania żadnych danych systemowi POS – nawet numeru konta bankowego. Dotyczy to zarówno płatności online, jak i tych realizowanych w sklepie. Dzięki temu płatność BLIK-iem stanowi

znacznie bezpieczniejszą opcję niż tradycyjna karta kredytowa. Jednak nawet przy tej formie płatności trzeba pamiętać o podstawowych środkach bezpieczeństwa.

**PODSTAWĄ I PIERWSZĄ
LINIĄ DOBREJ
OCHRONY POWINNA
BYĆ ODPOWIEDNIO
WYSZKOLONA KADRA
PRACOWNICZA.**



stwa. Nie należy udostępniać nikomu swojego kodu BLIK, szczególnie przez internetowe komunikatory. W sytuacji zgubienia telefonu należy niezwłocznie skontaktować się z bankiem w celu zamrożenia konta.

Aspekty cyberbezpieczeństwa zazwyczaj nie są priorytetem podczas codziennych czynności, szczególnie przy tak powtarzalnych jak płatność kartą. Jednak zagrożenie ze strony cyberprzestępców jest realne, a skutki udanego ataku na punkty sprzedaży mogą być poważne. Fortinet rekomenduje wdrażanie kompleksowych rozwiązań zabezpieczających systemy POS oraz monitorowanie ruchu sieciowego w celu wykrywania anomalii. Udana ataki na urządzenia point-of-sale mogą skutkować poważnymi szkodami finansowymi dla obu stron – firmy i klientów. Dlatego ich zabezpieczenie powinno być traktowane z najwyższą powagą.

Coraz więcej e-sklepów oferuje płatność za pomocą Click to Pay

Click to Pay to wspierany przez Mastercard i Visa globalny standard płatności kartą w internecie. Pozwala na szybkie, wygodne i bezpieczne zakupy online.

Dzięki Click to Pay proces płatności online odbywa się w kilka sekund i w każdym miejscu wygląda tak samo – bez względu na to, gdzie kupujemy i jaką kartą płacimy. Usługa jest dostępna u takich dostawców, jak AutoPay, PayU, Przelewy24 oraz Tpay. Trwają prace wdrożeniowe u pozostałych dostawców bramek płatniczych, agentów rozliczeniowych oraz dużych merchantów i platform e-commerce'owych.

Miłośnicy zakupów mogą skorzystać z tego rozwiązania w coraz większej liczbie e-sklepów. Click to Pay pozwala konsumentom dokonywać zakupów bez konieczności wpisywania danych i numeru karty przy każdym zamówieniu oraz jednocześnie zapewnia wysoki poziom bezpieczeństwa transakcji online. Rozwiązanie oparte jest na technologii tokenizacji danych karty, co oznacza, że rzeczywiste dane zastępowane są unikatowym tokenem, dzięki czemu są chronione. Tokenizacja uznawana jest aktualnie za najlepsze dostępne rozwiązanie zwiększające bezpieczeństwo płatności cyfrowych.

– Zdaniem konsumentów transakcje w internecie powinny być przede wszystkim szybkie, wygodne i bezpieczne. Najlepiej, aby odbywały się za pomocą jednego kliknięcia, w tle, nie wymagały żadnych dodatkowych czynności oraz były

powtarzalne, czyli odbywały się wszędzie i za każdym razem w taki sam sposób. I właśnie takie udogodnienia oferuje Click to Pay – komentuje Joanna Erdman, prezeska Fundacji Polska Bezgotówkowa.

Click to Pay to odpowiedź na potrzeby i oczekiwania konsumentów kupujących w sieci. Ich odsetek na przestrzeni ostatniej dekady wzrósł niemal dwukrotnie, a liczba zarejestrowanych sklepów internetowych powiększyła się dwa i pół raza – pokazują dane Izby Gospodarki Elektronicznej. Według prognoz polski rynek e-commerce do 2027 r. będzie wart 187 mld zł¹. Z punktu widzenia konsumentów, najważniejsze znaczenie w płatnościach internetowych ma szybkość, wygoda i bezpieczeństwo transakcji. Ponadto dla kupujących online kluczowym czynnikiem decydującym o dokonaniu pierwszego zakupu w internetowym sklepie, z którego wcześniej nie korzystali, jest dostępność łatwego sposobu płatności – potwierdziło to 21 proc.

respondentów w badaniu IAB. Polacy do tego stopnia przykładają wagę do sposobu płatności, że brak preferowanej formy płatności na stronie internetowej e-sklepu staje się częstym powodem porzucenia koszyka przez kupującego.

– Dzięki Click to Pay nie musimy zapamiętywać haseł ani wpisywać kodów bezpieczeństwa czy tracić czasu na drobiazgowo przepisywanie cyfr. To znaczne uproszczenie i skrócenie procesu zakupowego dla klientów, co również finalnie może przełożyć się na konwersję zakupów i wyniki sprzedażowe e-sklepów. Click to Pay nie tylko poprawia doświadczenia zakupowe konsumentów, ale także zapewnia bezpieczeństwo transakcji online, a ten aspekt dla kupujących na odległość ma priorytetowe znaczenie – podsumowuje Joanna Erdman.

Więcej informacji: <https://polska-bezgotowkowa.pl/dla-ciebie/click-to-pay/>

1. Źródło: Pwc.com

materiał partnera



Przyszłość nowych metod płatności

Mobilne transakcje, identyfikacja biometryczna czy płatności zbliżeniowe przestały być innowacją – stały się standardem. Za ich powszechnością stoi jednak złożona architektura technologiczna, która musi sprostać zarówno oczekiwaniom klientów, jak i wymaganiom regulacyjnym.

Od odporności systemów po ochronę wrażliwych danych – każde niedopatrzenie może mieć poważne konsekwencje. W jakim kierunku zmierza cyfrowa transformacja płatności i jakich decyzji wymaga od instytucji finansowych?

GLOBALNA PRESJA, LOKALNE DECYZJE

I kw. 2025 r. dobiega końca. Globalna gospodarka notuje umiarkowany wzrost, mierząc się jednocześnie z dużą niepewnością. Napięcia geopolityczne i zmienność w polityce wciąż stanowią istotne zagrożenia, skłaniając firmy do ponownej oceny modeli operacyjnych i łańcuchów dostaw. W sektorze bankowym wzrasta presja na zmianę – również ze względu na oczekiwania

klientów, którzy coraz częściej poszukują bezproblemowych, spersonalizowanych doświadczeń cyfrowych oraz realnych korzyści na każdym etapie obsługi.

Cyfrowa rewolucja w obszarze płatności wynika nie tylko z potrzeb użytkowników, ale także z coraz bardziej rygorystycznych przepisów. Organy nadzorcze – zarówno krajowe, jak i międzynarodowe – coraz wyraźniej określają priorytety w rozwoju systemów płatniczych: stawiają na przejrzystość, ochronę danych, interoperacyjność oraz eliminację opóźnień. Dla wielu banków i operatorów płatności oznacza to konieczność modernizacji infrastruktury oraz dostosowania się do regulacji, które nierzadko wyprzedzają aktualne możliwości technologiczne rynku.

NOWE METODY PŁATNOŚCI: SZYBKO, WYGODNIE I... RYZYKOWNIE

Najbardziej widoczną zmianą w krajobrazie płatności jest błyskawiczny rozwój przelewów A2A (account-to-account) oraz portfeli cyfrowych. Umożliwiają one realizację transakcji w czasie rzeczywistym, bez udziału tradycyjnych kart. Zyskują popularność dzięki wygodzie, niższym kosztom i bezpieczeństwu.

Jak pokazuje opracowany przez Capgemini „World Payments Report 2025”, udział płatności natychmiastowych w globalnym wolumenie transakcji ma wzrosnąć z 16 proc. w 2023 r. do 22 proc. w 2028 r. Portfele cyfrowe również zyskają na znaczeniu – prognoza mówi o wzroście z 5 do 8 proc. w tym





samym okresie. Spadek dotknie kart, których udział zmniejszy się z 57 do 50 proc.

– Rosnąca popularność płatności A2A może znacząco ograniczyć rozwój tradycyjnych kart – mówi Maciej Olszański, Local Head of Financial Services w Capgemini Polska. – Szacujemy, że nawet 15-25 proc. przyszłego wzrostu w tym segmencie może zostać przejęte przez te nowe rozwiązania. Najbardziej narażone są karty debetowe i przedpłacone.

Nie wszystkie regiony rozwijają się jednak w tym samym tempie. Brazylijski system Pix już dziś zapewnia szeroki dostęp do usług płatniczych – umożliwia natychmiastowe przelewy bez konieczności podawania numeru konta odbiorcy, często przy użyciu kodu QR. Powstał

z inicjatywy banku centralnego i ma na celu ograniczenie transakcji gotówkowych, oferując

**ZMIANA
TECHNOLOGICZNA
TO TYLKO CZĘŚĆ
UKŁADANKI.
RÓWNIE WAŻNE
JEST ZROZUMIENIE
ZMIENIAJĄCYCH
SIĘ OCZEKIWAŃ
KONSUMENTÓW.**

rując szybszą i tańszą alternatywę dla tradycyjnych metod płatności. W Azji Indie, Hong-

kong i Singapur rozwijają własne, zaawansowane systemy, które zmieniają sposób, w jaki konsumenci korzystają z usług finansowych. UPI w Indiach integruje konta z różnych banków w jednej aplikacji i pozwala na natychmiastowe przelewy między rachunkami bez konieczności korzystania z kart czy systemu SWIFT. FPS w Hongkongu to bezpłatny system dostępny 24/7, umożliwiający płatności m.in. na numer telefonu, adres e-mail czy kod QR. Z kolei PayNow w Singapurze pozwala przysyłać środki w czasie rzeczywistym przy użyciu numeru telefonu, numeru NRIC lub wirtualnego identyfikatora płatniczego – bez potrzeby ujawniania danych konta odbiorcy. Tymczasem Europa i USA dopiero nadrobiają zaległości.



TECHNOLOGIA TO NIE WSZYSTKO – KLIENT W CENTRUM UWAGI

Zmiana technologiczna to tylko część układanki. Równie ważne jest zrozumienie zmieniających się oczekiwań konsumentów. Istotne są emocje, potrzeby i styl życia użytkownika. Tu z pomocą przychodzi model wzrostu typu flywheel, oparty na tworzeniu cyklu pozytywnych doświadczeń klienta: od przyciągnięcia uwagi przez aktywizację aż po budowanie lojalności. Kluczowe jest eliminowanie barier – skomplikowanych procesów onboardingu, nieintuicyjnych interfejsów czy zbyt ogólnych ofert.

– Raport „World Retail Banking 2025” podkreśla siłę modelu wzrostu opartego na podejściu skoncentrowanym na użytkowniku, w którym kluczowe znaczenie ma synergia pomiędzy precyzyjnie dobraną komunikacją a ofertą dostosowaną do oczeki-

wań i aspiracji konkretnych grup odbiorców. Aż 88 proc. liderów bankowości na świecie wskazuje rozbudowany ekosystem nagród jako najskuteczniejsze narzędzie zwiększania zaangażowania i lo-

INSTYTUCJE FINANSOWE MUSZĄ ZROZUMIEĆ, ŻE WYGODA, DOSTĘPNOŚĆ I PROSTOTA SĄ DZIŚ TAK SAMO WAŻNE JAK BEZPIECZEŃSTWO I FUNKCJONALNOŚĆ.

jalności klientów – komentuje Maciej Olszański.

Instytucje finansowe muszą zrozumieć, że wygoda, dostępność

i prostota są dziś tak samo ważne jak bezpieczeństwo i funkcjonalność. Tylko całościowe podejście może zapewnić stabilny rozwój i silne relacje z klientami.

NOWA LOJALNOŚĆ: PARTNERSTWA, EMOCJE I DANE

Programy lojalnościowe również przechodzą transformację. Tradycyjne punkty i rabaty przestają wystarczać. Klienci szukają wartości, która odpowiada ich stylowi życia – czy to w formie elastycznych zniżek, ekskluzywnych wydarzeń, czy spersonalizowanych doświadczeń.

– Dzisiejsza lojalność budowana jest na trzech filarach: partnerstwach z markami, ofercie premium i personalizacji opartej na danych – zauważa Maciej Olszański – To połączenie, które pozwala tworzyć kompleksowe programy angażujące użytkowników. Współpraca z cenionymi partnerami umożli-

liwia oferowanie korzyści wykraczających poza klasyczne rozwiązania bankowe. Dostęp do ekskluzywnych doświadczeń buduje poczucie wyróżnienia, a personalizacja – oparta na analizie zachowań i preferencji – sprawia, że klient otrzymuje dokładnie to, czego potrzebuje, zanim sam zdąży to wyartykułować. W efekcie lojalność nie jest już nagrodą za zakup, ale konsekwencją dobrze zaprojektowanej, długofalowej relacji.

Na rynku coraz częściej pojawiają się rozwiązania umożliwiające automatyczny zwrot części wydatków na konto inwestycyjne lub oszczędnościowe, wspierające budowanie bezpieczeństwa finansowego. Popular-

ność zyskują także ekologiczne karty wykonane z materiałów pochodzących z recyklingu czy programy lojalnościowe powiązane z inicjatywami społecznymi. Równolegle rozwijają się usługi pozwalające elastycznie rozłożyć w czasie płatności za opiekę zdrowotną, zabiegi medycyny estetycznej, wizyty u specjalistów czy leczenie zwierząt domowych – często w modelu ratałnym, z preferencyjnymi warunkami.

To najlepszy dowód na to, że lojalność nie opiera się już na rabatach – dziś jest narzędziem do budowania zaangażowania i zaufania, które może mieć wymierny wpływ na postrzeganie całej oferty.

CZY SEKTOR FINANSOWY NADĄŻY ZA TEMPEM ZMIAN?

Aby utrzymać swoją pozycję, instytucje finansowe muszą nie tylko wdrażać nowe technologie, ale przede wszystkim projektować kompleksowe doświadczenia klienta. Kluczowe będą elastyczność, szybka reakcja na zmiany i inwestycje w dane oraz AI, które pozwolą zrozumieć potrzeby klientów lepiej niż kiedykolwiek wcześniej.

Transformacja trwa – i nie czeka na spóźnionych. Ci, którzy zainwestują dziś w zwinność, personalizację i budowanie wartości w każdym punkcie kontaktu z użytkownikiem, zyskają przewagę nie tylko technologiczną, ale i relacyjną.

Bezpieczne płatności zaczynają się od jakości obsługi

W świecie cyfrowej gospodarki bezpieczeństwo płatności to nie tylko kwestia technologii, ale także skutecznego wsparcia użytkownika. Dlatego eService – największy agent rozliczeniowy w Polsce – od lat inwestuje w jakość serwisu i niezawodność rozwiązań płatniczych.

Firma jako jedyna w branży dysponuje własną siecią mobilnych serwisantów oraz całodobowym Centrum Obsługi Akceptantów działającym także w weekendy i święta.

Potwierdzeniem skuteczności wdrażanych standardów jest certyfikat PCI P2PE – najbardziej zaawansowany system zabezpieczeń danych kartowych. W 2024 r. eService uzyskał jego najnowszą wersję (v3.1), rozszerzając zakres o kolejne urządzenia i aplikacje. Firma posia-

da także certyfikaty ISO 9001 i ISO 18 295 obejmujące zarówno jakość procesów, jak i obsługę klientów.

ZAUFANIE KLIENTÓW BUDOWANE PRZEZ DEKADY

eService działa już 25 lat, obsługuje ponad 0,5 mln terminali i przetwarza do 2 mln transakcji na godzinę. Dzięki połączeniu globalnego know-how (Global Payments, PKO BP) z lokalnym wsparciem firma nie tylko dostarcza rozwiązania płatnicze, ale realnie

wspiera przedsiębiorców wtedy, gdy tego najbardziej potrzebują. Bezpieczeństwo transakcji, szybka pomoc techniczna i sprawna obsługa klienta to fundamenty, na których eService buduje swoją pozycję. Dzięki nim każdego dnia miliony Polaków mogą płacić wygodnie i bez obaw – w sklepie, online i w podróży.



material partnera