***Kontakt dla prasy:***

*Agnieszka Juraszczyk*

*+48 883 357 638*

*E-mail:* *agnieszka.juraszczyk@capgemini.com*

***Kontakt dla prasy:***

*Aleksandra Witkowska*

*+48 693 407 831*

*E-mail:* *aleksandra.witkowska@linkleaders.pl*

**Metaverse – nowe doświadczenie cyfrowe czy nowa skala zagrożenia?**

**Przyspieszając połączenie świata fizycznego ze światem cyfrowym, Metaverse może zaoferować nam wiele nowych sposobów doświadczania – w pracy, domu czy podczas zabawy. Technologia ta reprezentuje kolejny etap rozwoju, umożliwiając miliardom ludzi łączenie się w wirtualnych światach i doświadczanie prawdziwych emocji. Te publiczne i prywatne zdecentralizowane wirtualne przestrzenie będą budować doświadczenia klientów czy pracowników w sposób cyfrowy – np. poprzez kreowanie poczucia obecności, możliwość mówienia, wykonywania gestów, odczuwania dotyku, a nawet zapachu. Brzmi dobrze, ale to zjawisko nie jest pozbawione wad i realnych zagrożeń, m.in. w zakresie przestępstw finansowych.**

Nazwa Metaverse powstała od greckiego meta – „poza” lub „przekraczający” – i wszechświata. Świat wykraczający poza ten, w którym żyjemy. Eksperci stale podejmują szacunki dotyczące prognozowanego wzrostu rynku Metaverse w najbliższych latach. Właściwie wszyscy analitycy zgadzają się, że wzrost do końca dekady będzie znaczący, choć liczby się wahają. Jak wskazuje Metaverse Insider[[1]](#footnote-1), wartość ta do 2030 roku może stanowić od 700 miliardów USD aż do 13 bilionów USD. Olbrzymia skala tego zjawiska sprawia jednak, że rosną także zagrożenia.

**Wirtualna przestępczość, ale realne zagrożenia**

Metaverse staje się przestrzenią, w której ludzie z różnych środowisk mogą się spotykać i spędzać wolny czas. Ten nowy sposób gromadzenia się w wirtualnym świecie tworzy nowe metody prowadzenia działalności gospodarczej – umożliwiając jej użytkownikom m.in. prowadzenie sprzedaży. W Metaverse dochodzi do wymiany dóbr – można kupować choćby bilety na wirtualne wydarzenia czy nawet grunty i wiele innych rzeczy oraz usług – opłacanych kryptowalutami. W tej sytuacji konieczne są niezbędne zabezpieczenia, takie jak dla przykładu rozwiązania z zakresu KYC (ang. Know Your Customer - poznaj swojego klienta), czy AML (ang. Anti-Money Laundering, przeciwdziałające praniu brudnych pieniędzy). Pozwalają one zachować ostrożność, jaką muszą utrzymywać instytucje finansowe lub firmy, by móc identyfikować swoich klientów i bezpiecznie przeprowadzać procesy finansowe. Procedury te pomagają w sprawdzeniu tożsamości klienta, prowadzonej przez niego działalności gospodarczej i ocenie jego wiarygodności.

* *Jednym z największych problemów z jakimi muszą mierzyć się specjaliści AML, jest możliwość korzystania przez przestępców z wielu zdecentralizowanych rynków, zarówno w ramach samego Metaverse, jak i na styku świata wirtualnego i realnego. Na tak wysoce zdecentralizowanych platformach i przy braku centralnych organów nadzoru, śledzenie osób zajmujących się praniem brudnych pieniędzy jest niezwykle trudnym zadaniem. Podstawowym środkiem ochrony przed cyber-zagrożeniami w tym obszarze, są ścisłe kontrole już etapie dołączania użytkownika do platformy. Dlatego mówimy o konieczności implementacji polityk z obszaru KYC, mających za zadanie umożliwienie identyfikacji źródła pieniędzy, które są wykorzystywane do zakupu wirtualnej waluty. Dzięki ich prawidłowemu wdrożeniu jesteśmy w stanie zweryfikować prawdziwą tożsamość użytkowników oraz na czas rozpoznać podejrzaną transakcję, a finalnie uniemożliwić popełnienie przestępstwa – także w Metaverse. Brak zabezpieczeń generuje duże straty, zarówno finansowe jak i wizerunkowe. Dlatego w interesie firm działających w Metaverse jest korzystanie z nowoczesnych rozwiązań, które pomagają powstrzymać przestępców –* mówi **Marcel Pawlak, Senior Manager praktyki AML/KYC w Capgemini Invent.**

Metaverse daje użytkownikom skalę możliwości większą niż dotychczas dostępne sieci społecznościowe. Nic więc dziwnego, że do tego świata wkracza także przestępczość finansowa – duże możliwości, jakie daje platforma umożliwiają działanie także cyberprzestępcom. Aby temu przeciwdziałać, Unia Europejska podejmuje już pierwsze próby wprowadzenia pewnych regulacji. UE wskazuje, że oszustwa w Metaverse nie tylko są zagrożeniem dla użytkowników, wzbogacają grupy przestępcze, ale także ograniczają rozwój tego rynku – z uwagi na rodzące się obawy użytkowników.

**O jakich zagrożeniach mowa?**

Z uwagi na wspomniane niedoskonałości, w Metaverse występuje wysokie ryzyko prania brudnych pieniędzy. Platformy internetowe umożliwiające wymianę dóbr i kryptowalut mogą być użyte jako kanał do wykorzystywania nielegalnych funduszy czy nawet finansowania terroryzmu.

Ale to nie wszystko. Do czynienia mamy także z oszustwami związanymi z wyłudzaniem informacji, czyli phishingiem. Opierają się one np. o fałszywe strony internetowe, zaprojektowane w celu wyłudzania środków finansowych od internautów. Przykładowo cyberprzestępcy wykorzystują linki phishingowe „zaszyte” w imitacji panelu logowania dostawcy e-portfela. Wprowadzają one w błąd użytkownika, w rzeczywistości wysyłając jego dane do oszustów, którzy następnie są w stanie pobrać środki z wyłudzonego konta. Linki phishingowe nie są jednak jedyną metodą stosowaną przez cyberprzestępców. W tym środowisku łatwo jest wykorzystać także socjotechnikę – wzbudzanie zaufania użytkowników podczas podszywania się pod oficjalne projekty Metaverse. Przestępcy stosujący tę metodę są w stanie wyłudzić dane podczas rozmowy z użytkownikiem, nakłaniając do kliknięcia w dane miejsce lub przesłania środków na konto, które podaje się jako oficjalne.

Użytkownicy Metaverse muszą chronić się przed wieloma możliwymi zagrożeniami. Kradzieży kryptowalut można dokonać także poprzez wykorzystanie złośliwego oprogramowania, czyli tzw. ransomware, atakującego portfele cyfrowe. Ransomware jest jednym z najbardziej znanych zagrożeń dla naszego cyberbezpieczeństwa, które niestety jest też coraz powszechniej wykorzystywane w Metaverse, z uwagi na sposób, w jaki skonstruowane są te platformy (złożona sieć inteligentnych kontraktów). Ten wysoki poziom skomplikowania kodu, zasobów i usług w Metaverse prowadzi do powstawania luk, które cyberprzestępcy są w stanie zidentyfikować i wykorzystać.

* *Metaverse to nowe zjawisko i wielu konsumentów nie posiada jeszcze pełnej wiedzy na jego temat. To z kolei chętnie wykorzystują oszuści. Zgodnie z badaniami przeprowadzonymi przez Interpol możemy spodziewać się ponad 70% wzrostu cyberprzestępstw w ciągu najbliższych kilku lat. Aby im zapobiec, użytkownicy Metaverse powinni stosować jak najwięcej zabezpieczeń, takich jak choćby dwuetapowa autoryzacja tożsamości, pozwalająca lepiej chronić wirtualne konta. W raz z rozwojem nowych technologii zmienia się także podejście przestępców. Stosują oni już nie tylko ataki phishingowe ale również dopuszczają się oszustw wykorzystujących NFT oraz Smart Contracts. Aktualnie każdy, kto posiada wiedzę o tworzeniu blockchain, może intencjonalnie tworzyć kod z lukami w zabezpieczeniach. Tego typu oszustwa są szczególnie problematyczne, ponieważ transakcje w blockchain nie mogą zostać cofnięte. Zanim dokonamy płatności w Metaverse, powinniśmy każdorazowo i najlepiej, jak to możliwe sprawdzać operatora platformy, z którą przeprowadzamy transakcję. Zachowujmy ostrożność, która może uchronić nas przed oszustami –* dodaje **Marcel Pawlak, Senior Manager praktyki AML/KYC w Capgemini Invent.**

**Edukacja i współpraca kluczem do bezpiecznego rozwoju**

Światowe Forum Ekonomiczne prognozuje, że do 2026 roku 25% ludzi na świecie będzie spędzać co najmniej godzinę dziennie w Metaverse — a to naraża ich na niezliczone przestępstwa. Kradzieże aktywów wirtualnych to ryzyko, na które będą narażeni wszyscy użytkownicy tej wirtualnej przestrzeni.

Kluczem do bezpiecznego i odpowiedzialnego korzystania z Metaverse jest edukacja. Jako osoby dorosłe mamy obowiązek przekazywania informacji młodszym pokoleniom, które niejednokrotnie będą wchodzić w świat Metaverse coraz wcześniej. Pamiętajmy jednak, że konieczność edukowania nie dotyczy wyłącznie dzieci czy młodzieży, taką wiedzą należy dzielić się na co dzień ze wszystkimi użytkownikami platform. Muszą oni być świadomi, że uczestnictwo w każdej nowej technologii czyni ich potencjalnym celem przestępców. Tę rolę powinni podjąć rządzący oraz świadome i zaawansowane technologicznie organizacje. Działania informujące powinny z kolei podkreślać o czym należy pamiętać korzystając z Metaverse, na co zwracać uwagę, jakie zabezpieczenia stosować i jakie są najlepsze praktyki, które pozwolą nam pozostać bezpiecznymi w tych nowych, zaawansowanych platformach.

Także firmy pracujące w Metaverse muszą być odpowiednio przygotowane pod kątem cyberbezpieczeństwa i na wczesnym etapie rozpoczynać współpracę ze swoimi zespołami ds. bezpieczeństwa i zabezpieczeń. To wymaga dodatkowo wyszkolenia programistów w zakresie zagrożeń, jakie niosą te nowe platformy oraz wielokrotnego testowania przed włączeniem się w ten nowy, wirtualny świat. Odpowiedzialność jednak nie leży wyłącznie w rękach organizacji technologicznych, a przede wszystkim w rękach rządzących. Światowi liderzy muszą zaangażować się w rozwój polityk regulujących Metaverse, co nie będzie łatwym zadaniem, ponieważ po pierwsze, technologia rozwija się bardzo szybko, a po drugie – regulacje należy wprowadzać w taki sposób, by jednocześnie nie doprowadzić do zahamowania rozwoju technologii.

Wszystko to musi prowadzić do wspólnego celu: bezpiecznego eksplorowania możliwości, jakie zyskujemy dzięki innowacjom i najnowszym technologiom.

**O Capgemini**

Capgemini to światowy lider w dziedzinie doradztwa w zakresie transformacji i zarządzania biznesem poprzez wykorzystanie mocy technologii. Celem Grupy jest dążenie do odpowiedzialnej społecznie, zintegrowanej i zrównoważonej przyszłości, w której potencjał ludzki jest wspierany nowymi technologiami. Capgemini jest odpowiedzialną i wielokulturową organizacją, liczącą ponad 350 000 pracowników zatrudnionych w ponad 50 krajach. Dzięki silnemu 55-letniemu dziedzictwu i szerokiej wiedzy branżowej cieszy się zaufaniem swoich klientów, a także jest zdolna kompleksowo zaspokoić ich potrzeby biznesowe: od strategii i projektowania rozwiązań po działania operacyjne napędzane przez dynamicznie rozwijający się i innowacyjny świat technologii chmury, danych, sztucznej inteligencji, łączności, oprogramowania, inżynierii cyfrowej i platform. W 2021 roku Grupa odnotowała globalne przychody w wysokości 18 miliardów euro.

Get The Future You Want | [www.capgemini.com](http://www.capgemini.com/#_blank)

1. <https://metaverseinsider.tech> [↑](#footnote-ref-1)