**Metaverse to zupełnie nowe zagrożenia**

**Od wirtualnych spotkań po wciągające doświadczenia klientów w 3D, a nawet wycieczki po nieruchomościach - Metaverse zmieni sposób, w jaki działają firmy. Jak przewiduje Gartner , do 2026 r. jedna czwarta z nas będzie spędzać w Metaverse co najmniej godzinę dziennie, pracując, robiąc zakupy, ucząc się czy przeglądając media społecznościowe. Niektóre marki, takie jak Nike i Coca-Cola, już teraz wykorzystują go do działań promocyjnych oraz zakupów. Przy tak dużym zamieszaniu wokół Metaverse, łatwo zrozumieć, dlaczego coraz więcej firm zaczyna tam robić interesy. Jednak czy myślą o ryzyku? Wojciech Głażewski z Check Point Software przygląda się zagrożeniom, które niesie z sobą Metaverse.**

Największą przeszkodą w zapewnieniu Metaverse bezpiecznego środowiska są jego fundamenty. Metaverse opiera się na technologii blockchain, w przypadku której już widzieliśmy poważne luki w zabezpieczeniach na rynkach NFT i platformach blockchain, takich jak [OpenSea](https://research.checkpoint.com/2021/check-point-research-prevents-theft-of-crypto-wallets-on-opensea-the-worlds-largest-nft-marketplace/) , [Rarible](https://research.checkpoint.com/2022/check-point-research-detects-vulnerability-in-the-rarible-nft-marketplace-preventing-risk-of-account-take-over-and-cryptocurrency-theft/) i [Everscale](https://research.checkpoint.com/2022/check-point-research-detects-vulnerability-in-the-everscale-blockchain-wallet-preventing-cryptocurrency-theft/) . Ze względu na ogromną ilość złośliwej aktywności, którą obserwujemy, uważamy, że nie minie wiele czasu, zanim zaczniemy dostrzegać pierwsze ataki w Metaverse. Najprawdopodobniej będą się opierać na autoryzacji i przejmowaniu kont użytkowników, więc spodziewamy się, że tożsamość i uwierzytelnianie będą znajdować się w centrum zainteresowań zarówno firm zabezpieczających, jak i hakerów.

Użytkownicy najprawdopodobniej będą chcieli posiadać wiele tożsamości w Metaverse – np. jedną do prowadzenia rozmów w pracy, a drugą do osobistych zakupów i rozrywki. To dodaje kolejną warstwę złożoności, ponieważ nie będzie istnieć ta jednak, potwierdzająca, że to na pewno my. Odpowiedzią może być ich powiązanie, ale czy blockchain pomoże nam wtedy zrozumieć, gdzie i z kim przeprowadzamy transakcje? To spore wyzwanie, a ponieważ technologie blockchain są zdecentralizowane i nieuregulowane, to kontrolowanie bezpieczeństwa wirtualnych aktywów lub zapobieganie praniu pieniędzy, są naprawdę bardzo trudne do wdrożenia.

**Przedefiniowanie rzeczywistości**

Kolejnym kluczowym wyzwaniem w zakresie bezpieczeństwa są bezpieczne przestrzenie potrzebne do prowadzenia działalności. Wyobraź sobie, że prowadzisz rozmowę Zoom lub Teams. To prywatna przestrzeń spotkań, prawda? Ale jak to będzie wyglądać w Metaverse? Skąd jednak wiemy, że krzesło, na którym ktoś siedzi, nie jest w rzeczywistości awatarem, będącym oszustem pośród uczestników? Możesz myśleć, że to niemożliwe, ale to wirtualny świat, w którym niemal wszystko jest możliwe. Musimy być w stanie rozróżnić, co jest prawdziwe, a co fałszywe, a posiadanie bezpiecznej przestrzeni do spotkań i transakcji będzie miało kluczowe znaczenie.

Kiedy Internet pojawił się po raz pierwszy, cyberprzestępcy wykorzystywali brak znajomości technologii przez przeciętnego człowieka, tworząc złośliwe witryny podszywające się pod banki w celu uzyskania danych finansowych. Takie oszustwa phishingowe wciąż się zdarzają, chociaż obecnie obserwujemy bardziej wyrafinowane formy socjotechniki. Metaverse jest jak zupełnie nowy Internet i wydaje się pewnym, że nieznajomość tej technologii zostanie wykorzystana.

Co ciekawe, każda transakcja, która ma miejsce na blockchainie, jest w pełni identyfikowalna, co będzie istotne, zwłaszcza jeśli chodzi o posiadanie ścieżek audytu dla decyzji biznesowych. Pozostaje jednak pytanie, w jaki sposób te informacje są przenoszone ze świata wirtualnego do fizycznego. Czy kontrakty Metaverse będą prawnie wiążące? A może uczestnicy Metaverse będą musieli spotkać się w świecie fizycznym, podpisując umowy, które następnie wdrażane będą ponownie w Metaverse? Jak zostanie to zabezpieczone?

Badacze odkrywali już luki bezpieczeństwa w projektach blockchain i kryptowalut, które są częścią Metaverse. Luki w zabezpieczeniach wykorzystywane przez cyberprzestępców związane są zwykle z inteligentnymi kontraktami, które umożliwiają hakerom wykorzystywanie i osuszanie platform kryptograficznych lub z zabezpieczeniami aplikacji na platformach blockchain, które umożliwiają hakerom atakowanie i przejmowanie portfeli użytkowników. Istnieje niebezpieczeństwo, że liczne firmy rzucą się na oślep do Metaverse bez rozważenia tego typu implikacji.

Wiele obaw związanych z bezpieczeństwem w Metaverse potęguje ogromny niedobór wykwalifikowanych pracownióków w sektorze cyberbezpieczeństwa. Według [badania 2021 (ISC)² Cybersecurity Workforce Study](https://www.isc2.org/-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx) , brakuje nam prawie 3 milionów specjalistów ds. cyberbezpieczeństwa, a obecna globalna siła robocza bezpieczeństwa cybernetycznego powinna urosnąć o 65%, aby skutecznie chronić krytyczne zasoby organizacji. Ten odsetek będzie prawdopodobnie znacznie wyższy, jeśli weźmiemy pod uwagę również nowy wirtualny świat.

**Czy warto?**

Inne zagrożenia cybernetyczne w Metaverse to m.in. potencjalne cyberataki za pomocą podatnych urządzeń AR/VR, jako drogi wejścia dla ewoluujących złośliwych programów i naruszeń danych. Urządzenia te z natury gromadzą duże ilości danych i informacji o użytkownikach, takich jak dane biometryczne, co czyni je atrakcyjnymi dla hakerów. Wśród sceptyków Metaverse coraz częściej pojawiają się również obawy dotyczące właśnie prywatności danych.

Być może zastanawiasz się, po co zawracać sobie głowę tą technologią, jeśli wiąże się ona z tak wieloma zagrożeniami? Metaverse to przyszłość, dlatego już dziś powinniśmy rozmawiać i myśleć o jego słabych punktach. Niestety każda firma (bez względu na wielkość), która tego nie robi, może znaleźć się w miejscu, w którym angażuje się w procesy narażające firmę na ryzyko. A można przecież do tego podchodzić powoli, tak jak miało to miejsce z rozwiązaniami w chmurze.