Hrozba budoucnosti? Útoky na metaverse (fiktivní vesmír)

2.4.2022 - Ladislav Procházka | INFOPROFI GROUP s.r.o.

Představte si, že diskutujete se svým šéfem o důvěrné mnohamilionové dohodě. Rozhovor končí a oba odejdete. O chvíli později se oba znovu setkáte a navážete svůj dřívější rozhovor – ale váš šéf si na dohodu absolutně nepamatuje.

Co se právě stalo?

„Ve fiktivním vesmíru to může znamenat, že jste se stali obětí hacknutého avatara nebo deepfake“, řekl Prabhu Ram, vedoucí průmyslové zpravodajské skupiny v CyberMedia Research, výzkumné a konzultační firmě. Deepfakes odkazují na zmanipulované digitální postavy, které vypadají nebo znějí jako někdo jiný.

Metaverze vyvolala v posledních měsících značný rozruch a společnosti jako Meta, dříve známá jako Facebook, a Ralph Lauren, spěchaly, aby se ve vývoji dostaly do popředí. Ale pokud nebudou řešena rizika kybernetické bezpečnosti v metaverse, nemusí tyto společnosti zaznamenat úspěch, ve který doufají. Kyberzločin v reálném světě je již stále více na denním pořádku.

Metaverse je síť 3D virtuálních světů zaměřených na sociální spojení. Ve futurismu a sci-fi je často popisován jako hypotetická iterace internetu jako jediného univerzálního virtuálního světa, který je

usnadněn používáním náhlavních souprav pro virtuální a rozšířenou realitu.

Společnost Check Point, zabývající se kybernetickou bezpečností, oznámila v roce 2021 více jak 50% nárůst celkových útoků za týden na podnikové sítě ve srovnání s rokem 2020. Jak podniky spěchají se „zavěšováním své vlajky do metavesmíru“, ne všichni si možná uvědomují všechna nebezpečí tohoto nového světa.

JPMorgan vydala v únoru bílou knihu, která uznala identifikaci uživatele a ochranu soukromí jako důležité prvky pro interakce a transakce v metavesmíru.„Ověřitelné přihlašovací údaje by měly být snadno strukturovány, aby umožnily snazší identifikaci členů komunity nebo týmu nebo umožnily konfigurovatelný přístup k různým umístěním a zkušenostem virtuálního světa,“ uvádí se v bílé knize. Lidé se dívají na blockchain, aby identifikovali uživatele, nebo „pomocí tokenů, které by mohla přiřadit organizace, nebo biometriky v náhlavní soupravě, kterou nosíte, takže existuje taková úroveň důvěry, takže vlastně víte, s kým mluvíte. Další možností je mít nad hlavami avatarů „malé vykřičníky“, které signalizují, že je člověk nedůvěryhodný.

Uživatelé zanechávají digitální stopy i ve virtuální realitě, může zde tedy docházet k narušení soukromí uživatelů ze strany technologických společností.Když uživatelé nosí zařízení, jako jsou náhlavní soupravy pro virtuální realitu, organizace mohou shromažďovat data, jako je jejich pohyb hlavy a očí nebo jejich hlas, řekl Philip Rosedale, zakladatel Second Life, online světa, který lidem umožňuje virtuálně se scházet, jíst a nakupovat. „To znamená, že během několika sekund dokážeme identifikovat, že to zařízení máte přesně na sobě. To je velmi vážný potenciální problém ochrany soukromí pro virtuální svět,“ řekl.

Spoluzakladatel Microsoftu Bill Gates předpověděl, že během příštích dvou až tří let se většina virtuálních setkání přesune do metaverze.

Co se dá dělat?

Aby podniky mohly bezpečně fungovat v metaverzu, je důležité dobře vyškolit zaměstnance. Nejslabším místem v jakékoli organizaci z hlediska kybernetické bezpečnosti je uživatel.Uživatelé budou muset mít možnost používat „síť důvěry“ k výměně informací s ostatními, aby si mohli snadněji vybudovat důvěru. Identifikace lidí, kterým důvěřujete, a sdílení těchto informací s dalšími důvěryhodnými lidmi vám umožní posoudit, zda máte společné přátele s někým novým.

https://www.cnbc.com/video/2022/02/09/virtual-world-firm-says-metaverse-should-be-legislated-like-real-world.html