

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **3** ze dne **11.1.2022**

JAK SI CHRÁNIT SVOJI DIGITÁLNÍ IDENTITU V NOVÉM METASVĚTĚ?

Po přejmenování společnosti Facebook na Meta a oznámení Marka Zuckerberga se rozběhla celosvětová debata o nových virtuálních světech – metaverzech. Nadnárodní firmy, a dokonce i státy plánují, že budou v tomto digitálním prostředí otevírat svoje pobočky a realizovat různé projekty. Během několika posledních let je termín „metaverzum“ velmi často zmiňován v souvislosti s různými hrami a firmami, například Fortnite, Microsoft, Roblox, Minecraft, Balenciaga a Nike, i ve spojení s technologiemi rozšířené reality (AR) a virtuální reality (VR).

Označení „Metaverse“ použil spisovatel science fiction Neil Stevenson ve svém kyberpunkovém románu Snow Crash vydaném v roce 1992. Stevensonovo metaverzum představuje další vývojový stupeň internetu – veřejný digitální svět, který kombinuje „fyzickou“ realitu s rozšířenou a virtuální realitou.

Matrix se stává realitou, i se všemi jeho nešvary

Lidé mohou do metaverza vstupovat tak jako v on-line hrách v podobě virtuálních postav (avatarů) a dělat vše, jako by byli v reálném světě – vyhledávat informace, komunikovat, nakupovat nebo pracovat, ale také uniknout z běžné reality a žít ve vysněném virtuálním vesmíru. Lidský avatar v metaverzu může být čímkoli a vlastnit cokoli chce, a ani smrt nemá stejný význam jako v reálném světě.

Některé příklady plnohodnotných digitálních světů v populární kultuře najdeme třeba v trilogii Matrix nebo v knize a ve filmu Ready Player One, kde se obdobou metaverza stala multiplayerová on-line hra OASIS.

Kromě digitálních světů se virtuální obrazy již postupně stávají součástí dnešní reality. V USA byla spuštěna show Alter Ego, v níž soutěžící zpívají v zákulisí a technologie motion capture vytváří jejich digitální avatary, kteří se objevují místo nich na scéně.

Lidé, pro které se metaverzum stane v budoucnu součástí jejich životů, by se měli zamyslet nad bezpečností digitálních avatarů a možnými hrozbami souvisejícími s virtuálními světy:

1. Krádež identity nebo účtu podobně jako na existujících sociálních sítích nebo v multiplayerových hrách. Možné následky jsou:
 - Ztráta nebo odcizení osobních údajů (například korespondence nebo její obdoby v metasvětě, což může vést například k vydírání).
 - Krádež virtuálních platidel, skutečných peněz nebo kryptoměn z karet a digitálních peněženek spojených s účtem nebo odcizení drahých virtuálních předmětů, například skinů nebo oblečení.
 - Využívání avatara k podvodům (scénáře, kdy jsou přátelé nebo členové rodiny žádáni o půjčení peněz).
2. Sociální inženýrství – Podobně jako například v seznamovacích aplikacích, a jistě vzniknou i jejich metaverzové obdoby, nemusí být lidé ve virtuální realitě těmi, za koho se vydávají, nebo nemusí mít dobré úmysly.

Možné problémy:

- Catfishing (vytváření falešné identity pro záměrné oklamání jiných lidí)

MEATEST spol. s r.o. - sdělení pověřence pro ochranu osobních údajů číslo **3** ze dne **11.1.2022**

- Stalking (pronásledování a obtěžování) a doxing (neoprávněné zveřejnění soukromých informací). Společnosti Kaspersky a Endtab.org připravily kurz, jak se před doxingem chránit nebo jak se vypořádat s jeho následky.
 - Jiná nebezpečí při přechodu z virtuálního do reálného světa.
3. Ohrožení soukromí – Metaverza jsou jako sociální média, jen ve virtuální realitě, a proto musí být uživatelé ostražití a dobře chránit svoje osobní údaje (například údaje z pasu nebo číslo letenky).
 4. Problémy spojené s blockchainem. Pokud je identita uživatele postavena na digitální peněženice, jako je tomu v digitálním světě Decentraland, pak je třeba ji chránit.
 5. Aktivními uživateli metaverza se mohou stát i děti. Jedním z významných příkladů je platforma Roblox, která se mezi dětmi dlouhodobě drží na vrcholu nejoblíbenějších her. Je proto také důležité předvídat možné problémy a chránit děti před pachateli trestné činnosti při setkáních v prostředí VR.

zdroj: Avcentrum ČR