ANDORRA DIGITAL

ANC-AD
Agència Nacional de Ciberseguretat d'Andorra

Informe de Ciber-Intel·ligència

La ciberseguretat i el metavers

06/02/2023

FITXA DEL DOCUMENT

Títol del document	La ciberseguretat i el metavers

Versió	Redactat/Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	ANC-AD	ANC-AD	17/02/2023	17/02/2023

Registre de canvis			
Versió	Pàgines	Data de modificació	Motiu del canvi

Propietari del document	ANC-AD

ÍNDEX

1. INTRODUCCIÓ 4
2. METODOLOGIA 5
3. EL METAVERS 6
3.1 QUÈ ÉS EL METAVERS? 6
3.2 QUI HA DESENVOLUPAT EL METAVERS? 7
3.3 CARACTERÍSTIQUES DEL METAVERS 7
3.4 ACCIONS D'EMPRESES AL METAVERS 8
3.5 REGULACIÓ AL METAVERS 10
3.6 OPEN METAVERSE ALLIANCE (OMA3) 11
4. LA CIBERSEGURETAT AL METAVERS 12
4.1 DARRERS ESDEVENIMENTS 12
4.2 FORMES D'ATAC EMPRATS 13
4.3 ACTORS D'AMENAÇA 14
4.4 TIPOLOGIA DE CIBERATACS 15
5. REPTES I DESAFIAMENTS DE LA SEGURETAT AL METAVERS 16
6. RECOMANACIONS 18
7. GLOSSARI 20
CLÀUSULA DE CONFIDENCIALITAT 23

1. INTRODUCCIÓ

El present informe té com a principal objectiu donar a conèixer el metavers i la importància de la ciberseguretat en aquest espai. La ciberseguretat i el metavers són dos temes estretament relacionats que s'estan tornant cada vegada més importants a mesura que la tecnologia avança.

El metavers, també conegut com a espais de realitat virtual, és un terme emprat per descriure un lloc tridimensional compartit on els usuaris poden interactuar entre ells amb l'aparença d'avatars. A mesura que el metavers s'ha tornat cada cop més popular, és important considerar les implicacions de seguretat en aquesta inèdita tecnologia.

Per molts, el metavers és l'inici de la fi d'Internet tal com el coneixem donat que es tracta d'un gran pas a nivell tecnològic que de ben segur es troba amatent de revolucionar la nostra manera de treballar, consumir i relacionar-nos. No obstant això, per uns altres, tot això no són més que expectatives massa exagerades. De fet, hi ha els qui pensen que el metavers s'ha convertit en una de les grans decepcions dins del sector tecnològic a principis del 2023. Això ha ocorregut atès que hi ha hagut pèrdues milionàries en el negoci de la venda d'ulleres de realitat virtual, així com pels qui varen impulsar aquesta tecnologia. La principal prova del fracàs del metavers es troba en els resultats de Meta, la matriu de Facebook, una de les companyies que més va apostar per aquesta tecnologia.

Malgrat els seus detractors, podem afirmar que el metavers és una tecnologia en constant evolució i que té el potencial de revolucionar la forma en què interactuem i ens relacionem amb el món. En aquesta línia, considerem que és un tema rellevant perquè està en ple desenvolupament i la ciberseguretat resulta un element clau en aquesta nova tecnologia.

Entre les principals preocupacions amb el metavers, es troba la possibilitat que els ciberdelinqüents accedeixin a informació personal i robin les dades personals dels usuaris. Això podria incloure informació com a números de targetes de crèdit o d'identificació personal que podrien ser utilitzades pel furt d'identitat o altres activitats malicioses. Endemés, aquests infractors podrien emprar el metavers per a propagar *malware* o llançar atacs cibernètics contra altres usuaris o sistemes.

Una altra preocupació és la possibilitat que el metavers sigui utilitzat per activitats malintencionades com el ciberdelicte, espionatge o la guerra cibernètica. És probable que els ciberdelinqüents trobin maneres d'explotar la tecnologia pel seu propi benefici. Això podria incloure l'ús d'aquests espais virtuals per a dur a terme activitats il·lícites

com per exemple el blanqueig de capitals, el tràfic de drogues o fins i tot activitats terroristes.

2. METODOLOGIA

Aquest informe aplica els principis de Traffic Light Protocol (TLP). Es tracta d'un esquema creat per fomentar un millor intercanvi d'informació de caràcter delicat (però no classificada) en l'àmbit de la seguretat de la informació. A través d'aquest esquema, d'una forma àgil i senzilla, s'indica fins a on pot circular la informació més enllà del receptor en qüestió, i aquest ha de consultar a l'ANC-AD (Agència Nacional de Ciberseguretat d'Andorra) [https://www.anc.ad/] quan la informació necessiti ser distribuïda a tercers.

CODI	QUAN EMPRAR-LO	COM COMPARTIR-LO
TLP:RED	S'ha d'utilitzar TLP:RED quan la informació està limitada a persones concretes, i podria tenir impacte en la privacitat, reputació o operacions si és mal utilitzada.	Els receptors no han de compartir informació designada com TLP:RED amb cap tercer fora de l'àmbit on va ser exposada originalment.
TLP:AMBER	S'ha d'usar TLP:AMBER quan la informació requereix ser distribuïda de manera limitada, però suposa un risc per a la privacitat, reputació o operacions si és compartida fora de l'organització.	Els receptors poden compartir informació indicada com TLP:AMBER únicament amb membres de la seva pròpia organització que necessiten conèixer-la, i amb clients, proveïdors o associats que necessiten conèixer-la per a protegir-se a si mateixos o evitar danys. L'emissor pot especificar restriccions addicionals per a compartir aquesta informació.
TLP:GREEN	S'ha d'emprar TLP:GREEN quan la informació és útil per a totes les organitzacions que participen, així com amb tercers de la comunitat o el sector.	Els receptors poden compartir la informació indicada com TLP:GREEN amb organitzacions afiliades o membres del mateix sector, però mai a través de canals públics.
TLP:WHITE	S'ha d'utilitzar TLP:WHITE quan la informació no suposa cap risc de malsense ús, dins de les regles i procediments establerts per a la seva difusió pública.	La informació TLP:WHITE pot ser distribuïda restriccions, únicament subjecta a controls de Copyright.

3. EL METAVERS

En aquest apartat explicarem què és el metavers, els seus orígens, les seves característiques, la regulació i els reptes i desafiaments als quals s'enfronta.

3.1 Què és el metavers?

Etimològicament, «metavers» és una paraula formada a partir del prefix grec «meta» que significa "més enllà" i de la contracció del substantiu univers: «vers». No obstant això, encara no es té una definició precisa i clara atès que és un concepte que actualment es troba en procés de disseny i desenvolupament.

El metavers podria definir-se com una nova dimensió digital a la qual les persones accedeixen en forma d'avatar per fer gairebé tot el que fem en el món físic: comprar, vendre, produir, consumir, treballar, formar-se, jugar, divertir-se i socialitzar, però amb una experiència sensorial immersiva. En altres paraules, és la capacitat tecnològica de replicar el món físic a través del processament de dades i la hiperconnexió perquè aquesta realitat alternativa funcioni amb fluïdesa. En aquest sentit, la Ciberseguretat resulta un element de vital importància.

Per accedir al metavers necessitem dispositius especials com ara ulleres de realitat virtual o augmentada i auriculars que ens permeten interactuar amb els altres usuaris. A més de llegir i sentir informació en una pantalla, tal com estem acostumats amb les xarxes socials, podem interactuar amb aquest entorn digital de dues maneres gràcies a la tecnologia 3D:

- Realitat Virtual (RV): Un món compost per elements virtuals. Es tracta d'un espai alternatiu on els usuaris poden establir relacions, desenvolupar comerços, comunitats i dur a terme activitats juntament amb altres persones. Endemés, poden crear entorns i objectes que en el món tangible són impossibles.

- Realitat Augmentada (RA): Una realitat denominada com “mixta”, consisteix en la inclusió de mitjans audiovisuals 3D en l’entorn físic. La seva relació amb la tecnologia hologràfica permet observar objectes virtuals en 3D que existeixen en el món real i canviar l'aparença d'aquests modificant els seus colors i formes.

Cadascun dels usuaris té un avatar (el seu personatge dins el món virtual) per poder interrelacionar-se en diferents àmbits. Per exemple, un internauta podria interactuar amb els seus amics, treballar amb els seus companys, compartir contingut amb la seva parella, assistir a concerts, viatjar, etc. Això suposa una immersió íntegra en el món

digital en el qual els diferents espais (personals i laborals), així com els processos de consum i la manera en què ens comuniquem passarien a estar digitalitzats completament. En resum, moltes coses que necessitem fer mitjançant moviment físic serien realitzades per avatars en un món virtual o estarien a només un clic del nostre dispositiu mòbil.

3.2 Qui ha desenvolupat el metavers?

No es coneix amb exactitud quin fou l'origen del metavers, però sí que se sap quan es va començar a parlar d'ell. El terme «metavers» va ser encunyat per l'escriptor Neal Stephenson, qui a l'any 1992 va publicar la novel·la de ciència-ficció "Snow Crash" en la qual internet havia evolucionat cap a un món virtual anomenat metavers.

Cal destacar que no existeix només un metavers: S'han creat diversos d'ells a través de videojocs com per exemple Minecraft, Fortnite, Second Life o Els Sims. Mark Zuckerberg, per part seva, va presentar el novembre de 2021 el seu projecte de metavers, a través d'una transmissió en directe per YouTube. La creació d'aquest món virtual ha portat a canviar el nom de la companyia Facebook pel de Meta.

Actualment, les grans empreses tecnològiques estan participant activament en una cursa l'objectiu del qual és ser les creadores del millor metavers. La meta d'aquestes empreses és aconseguir un univers virtual i únic en 3D que integri tots els elements que existeixen en el món tangible i en l'intangible (oci, comunicació, consum, treball, etc.), la qual cosa es denomina com la "nova Internet". En aquesta línia, busquen desenvolupar l'eina virtual definitiva que abasti tant la Realitat Virtual com la Realitat Augmentada, i que permeti optimitzar l'activitat humana per cadascun dels elements assenyalats.

3.3 Característiques del metavers

A continuació, presentem les característiques principals del metavers:

- Ús de tecnologies al núvol, la Internet de les coses (IoT), el *big data* i la intel·ligència artificial (IA).
- Creació de la seva pròpia economia a través del pagament amb criptomonedes i els Non Fungible Tokens (NFT's). La criptografia serà la base de qualsevol mena de transacció.

- Nous formats d'ocupabilitat, emprenedoria i millora de la productivitat al treball. El metavers portarà amb ell la generació de nous llocs de treball i s'estima que els equips siguin més multidisciplinaris, més eficients i amb una major productivitat en la consecució de les tasques i assoliment dels objectius.

- Aposta per un món més sostenible. Si en un futur operem de manera continuada en aquest món virtual, reduirem molts dels nostres trasllats per via terrestre i estalviaríem en combustibles fòssils i altres recursos materials.

- Sistemes avançats en l'àmbit educacional i acadèmic. Amb el metavers es generaran espais de treball i estudi virtuals amb una gestió més eficaç. Això està alineat amb el que va succeir durant la pandèmia de la COVID-19 on vàrem adoptar mecanismes de treball com aules virtuals i processos interactius.

3.4 Accions d'empreses al metavers

És important conèixer les iniciatives de les empreses en el metavers a fi d'identificar quins sectors seran els més sensibles als ciberatacs. Entre els projectes de màrqueting i bránding en el metavers, destaquen els sectors de la venda al detall i el món de la moda, els esports i l'oci, el turisme i la restauració, i el sector automobilístic, entre altres.

Venda al detall i moda

El holding de moda Forever 21, amb marques filials com Forever, Heritage 1981 i Love 21; o també altres companyies tèxtils de renom com Nike, Ralph Lauren, o la matriu VF Corporation, que comercialitza marques com Vans, The North Face o Timberland, ja disposen dels seus propis espais virtuals a la plataforma multi-jugador «Roblox».

Inditex, per part seva, va presentar la seva pròpia aposta al metavers amb un conjunt de peces de Pull&Bear compatibles amb les aplicacions i jocs de la plataforma Ready Player Em. El projecte es va completar amb una experiència de màrqueting en Realitat Virtual amb les ulleres VR Quest 2, amb les quals l'avatar del consumidor podia provar-se peces de roba.

Un altre exemple del sector de la venda al detall al metavers és la "Metaverse Fashion Week", organitzada al metavers de Decentraland. Segons els organitzadors, més de 60 marques, artistes i dissenyadors van participar en les passarel·les virtuals del 2022. Entre les marques més destacades hi trobem: Dolce&Gabbana, Etro, Elie Saab, DUNDAS, i Nicholas Kirkwood.

Esports i oci

A l'Open d'Austràlia de Tenis del 2022, els organitzadors van fer una incursió al metavers de Decentraland amb una simulació virtual de Melbourne Park. L'objectiu de l'empresa va ser promoure l'*engagement* entre els seus gairebé 750.000 visitants, per as que també varen comercialitzar sis col·leccions de NFT's amb el disseny de les passades que s'han utilitzat des del 1970.

El club de futbol anglès Manchester City, un dels més actius en la venda de *Fan Tokens* pels seus aficionats, s'ha associat amb Sony per reconstruir digitalment l'Etihad Stadium (l'estadi on juga l'equip londinenc). Com a resultat, els fanàtics podran visitar l'estadi i veure el partit en viu des de la comoditat de la seva llar. A més, s'està estudiant la possibilitat que els fanàtics es reuneixin amb els seus ídols al metavers mitjançant avatars que poden interactuar entre si.

Els concerts al metavers també estan sent una de les fórmules més explotades per artistes i cantants. De la mà d'Epic Games, Travis Scott, Ariana Gran i el DJ Marshmello han participat en recitals virtuals al videojoc de Fortnite. Meta, per part seva, va organitzar a les acaballes del 2021 actuacions virtuals del raper Young Thug, el DJ David Guetta, i el duo de productors musicals The Chainsmokers a la seva plataforma per esdeveniments denominada com Horizon Venues.

Turisme i restauració

A Espanya, el projecte pilot "Benidorm Land", desenvolupat a la plataforma espanyola SIX3D, ofereix una visita virtual per conèixer la ciutat. La idea és anar sumant noves experiències com ara NFT's d'edificis emblemàtics de Benidorm, concursos de fotografia i que els concerts que se celebrin a la ciutat tinguin la seva rèplica al metavers.

Durant març de 2022, Wendy's va establir el «Wendyverse» a Meta's Horizon Worlds, la plataforma de realitat virtual de la companyia de xarxes socials. Aquí, els clients poden visitar un punt de venda virtual de Wendy's. El 15 de juny va anunciar la seva pròxima versió de «Wendyverse», en la qual s'hi afegeix un castell ple de jocs virtuals anomenat «Sunrise City» per promocionar el seu menú de desdejuni.

La cadena de menjar ràpid «Chipotle Mexican Grill» va llançar un menú al videojoc Roblox el 2022. Aquest es converteix en el primer restaurant a llançar un menú de menjar al metavers, amb el qual promet endinsar-se més a la Web 3.0.

Altres exemples en el sector inclouen la cadena d'hotels de Singapur Millennium Hotels al metavers de Decentraland, i el grup Regal Hotels de Hong Kong a Sandbox.

Altres empreses i accions dutes a terme al metavers

Altres sectors econòmics i empreses que realitzen campanyes de màrqueting al metavers serien la banca i els serveis financers així com signatures d'arquitectura i immobiliàries. La indústria sanitària també està començant a incorporar tecnologia de Realitat Augmentada per formar als seus interns i efectuar operacions.

3.5 Regulació al metavers

La privacitat al metavers serà un tema important donat que no existeix cap mena de regulació específica. Endemés, l'experiència del metavers és de caràcter universal i no es regeix sota cap mena de llei regional de protecció de dades com seria el Reglament General de Protecció de Dades (GDPR). En aquesta línia, podria generar conflictes respecte a les notificacions de violacions de dades.

Com sabem, les xarxes socials són un centre d'activitat de violacions pel que fa a dades personals. Per aquesta raó, és evident que el metavers esdevindrà una extensió d'aquesta problemàtica. Segons va informar Cointelegraph, les xarxes socials van ser responsables de més de mil milions de dòlars en pèrdues relacionades amb estafes de criptomonedes a l'any 2021.

Ben segur que aquestes noves xarxes portaran més riscs de privacitat. En aquesta línia, els ciberdelinqüents podran començar a distribuir aplicacions falses (amb un troià a l'interior) per tal d'infectar els telèfons de les víctimes amb finalitats malicioses. Altres perills estaran associats amb el robatori de dades i diners, així com les pàgines de *phishing* destinades a segrestar comptes a aquestes noves xarxes socials, tal com veurem més endavant. Per exemple, Meta - l'empresa abans coneguda com a Facebook - ha rebut moltes crítiques per la falta de protecció de dades dels usuaris al metavers i a la preocupació per la privacitat en la seva plataforma de xarxa social.

Ja s'han detectat casos de violació i d'abús d'avatars. Així doncs, l'abús i les agressions sexuals virtuals al metavers també s'estendran com a crims i no han de quedar impunes.

Un altre cas a tenir en compte és que les transaccions financeres realitzades a través d'avatars intel·ligents generaran dades, per la qual cosa sorgeixen preguntes sobre com

aquests han de processar-se i regular-se i quins contractes han d'existir per garantir la privacitat.

Caldria pensar en altres qüestions com si es crearà una ciber-legalitat específica pel metavers, o si s'executaran solucions de ciberseguretat a través d'una policia digital.

3.6 Open Metaverse Alliance (OMA3)

La suma d'esforços per construir i consolidar el metavers s'està donant entre les empreses d'aquest àmbit.

D'aquesta manera, neix l'1 de novembre del 2022, la Open Metaverse Alliance (OMA3). Es tracta d'un consorci format per les principals empreses natives del metavers: The Sandbox, Animoca Brands, Alien Worlds, Dapper Labs, Decentraland, MetaMetaverse, Space, SuperWorld, Upland, Voxels, Unstoppable Domains i Wivity.

OMA3 pretén garantir que els terrenys virtuals, els actius digitals, les idees i els serveis siguin altament interoperables entre plataformes i transparents per totes les comunitats. Des del llançament de la Open Metaverse Alliance (OMA3), 50 membres s'han registrat en aquesta organització sense ànim de lucre.

La visió d'OMA3 se centra en l'esforç per crear un metavers obert que també estigui gestionat per la comunitat i sigui descentralitzat, *indexable* i en el qual els usuaris puguin posseir i utilitzar els seus actius digitals (per exemple, NFT's), la seva identitat i la seva reputació entre múltiples plataformes. Així doncs, podem dir que la visió d'OMA3 és que els usuaris tinguin el control dels seus actius i no els propietaris de les plataformes, mentre que les idees i els serveis es basen en els fonaments de la descentralització i la interoperabilitat per optimitzar la llibertat individual i els resultats socials i econòmics, entre altres.

Segons Saro McKenna - directora general d'Alien Worlds i membre fundador d'OMA3 - s'estandarditzarà la col·laboració oberta pels metaversos a fi de garantir que els usuaris estiguin al centre de la construcció de la seva plataforma i de l'aplicació per controlar la seva identitat, el seu compte i els seus actius en propietat. OMA3 també s'encarregarà de produir normes tècniques, codi font obert, documentació sobre les millors pràctiques, promoció externa i enllaços amb l'ecosistema per donar suport a aquest propòsit.

4. LA CIBERSEGURETAT AL METAVERS

Es creu que el metavers canviarà la nostra forma de vida i tindrà conseqüències molt significatives en l'àmbit de la Ciberseguretat. No obstant això, no podrem saber-ho amb certesa fins que l'experiència es normalitzi, però sí que podem esmentar alguns aspectes rellevants. Entre ells es troben:

- Sorgiment de ciberatacs nous i desconeguts. Així mateix, es podria incrementar l'efectivitat d'uns certs ciberatacs que ja coneixem.
- Com ja s'ha esmentat, s'hauran de tenir en compte nous riscs per la privacitat de les persones. Per exemple, la proliferació de dades generades pel metavers amplifica els riscos associats com les filtracions de dades i els atacs de ciberseguretat. Garantir la privacitat és encara més important en el metavers perquè el comportament de l'usuari es pot capturar a un nivell més detallat que en el món físic. A més dels tipus d'atacs de programari maliciós que veiem en la Web 2.0, tenen més possibilitats de sofrir atacs Sybil on una identitat pot pretendre ser moltes identitats al mateix temps.
- Pel fet que es realitzen transaccions en un entorn virtual, existeixen riscos potencialment majors de robatori d'identitat i suplantació d'identitat. Es podrien donar casos de NFT'S falsificats i avatars falsos, que podrien revelar informació confidencial i permetre l'accés no desitjat a carteres de criptomonedes i estafes de *blockchain* d'organitzacions financeres falses.

En aquest apartat veurem els últims esdeveniments quant al Metavers i Ciberseguretat, les formes d'atac més utilitzades, els actors d'amenaça i la tipologia dels ciberatacs.

4.1 Darrers esdeveniments

A continuació, presentem alguns dels últims esdeveniments rellevants en l'àmbit de la ciberseguretat i el metavers:

- **Ciberdelictes en el metavers:** La popularitat del metavers ha atret els ciberdelinqüents, que han començat a perpetrar fraus i furts de dades en aquesta nova frontera digital.
- **Regulació de la ciberseguretat:** En resposta a aquests desafiaments, els governs i les organitzacions internacionals estan treballant en l'elaboració de lleis i normes per protegir la ciberseguretat i fomentar una cultura de seguretat en línia.

- **Desenvolupament de tecnologies de seguretat:** Les companyies tecnològiques estan invertint en el desenvolupament de tecnologies de seguretat més avançades per protegir els usuaris i les organitzacions contra els ciberatacs.

- A tall d'exemple, el govern del Regne Unit ja ha destacat la importància de la ciberseguretat i la governança en aquest entorn en el **Projecte de Llei de Seguretat en línia**.

4.2 Formes d'atac emprats

A continuació, esmentarem breument algunes de les formes d'atac utilitzats al metavers:

Abús virtual i agressió sexual

L'abús virtual i l'agressió sexual s'estendran als ecosistemes del metavers. S'han donat casos de violació i abús d'avatars i és probable que aquesta tendència continuï al llarg del 2023, atès que manca una regulació eficaç.

Furt d'actius virtuals

Les monedes virtuals i els objectes de valor dins del joc seran un dels principals objectius dels ciberdelinqüents, que tractaran de segrestar els comptes dels jugadors o d'enganyar-los perquè facin tractes fraudulents per lliurar-los actius virtuals de gran valor. La majoria dels jocs moderns han introduït alguna forma de monetització o suport de moneda digital, la qual cosa es convertirà en un punt de mira pels actors maliciosos.

Furt de dades i diners

Les noves formes de xarxes socials també portaran més riscs. El canvi a les xarxes socials basades en la realitat augmentada és un nou espai perquè els ciberdelinqüents puguin començar a distribuir falses aplicacions *troyanitzades* i infectar els dispositius amb fins maliciosos.

Les amenaces per les noves xarxes socials basades en la realitat augmentada i les plataformes del metavers són principalment el robatori de dades i diners, el *phishing*, i el *hackeig* de comptes.

4.3 Actors d'amenaça

S'han identificat als següents grups que estan actuant o podrien actuar en el metavers:

Hackers individuals o grups

Aquests actors busquen obtenir guanys econòmics o beneficis personals a través del robatori d'informació personal o financera dels usuaris.

Crim organitzat

Els grups criminals poden utilitzar el metavers per a dur a terme activitats il·legals, com la venda de drogues o el tràfic de persones.

Governs

Els governs poden emprar el metavers per espiar als ciutadans o per dur a terme accions de propaganda i desinformació.

Companyies

Algunes companyies poden usar el metavers per a espiar a la competència o per a recol·lectar informació sobre els consumidors.

Trolls i ciber-acosadors

Aquests actors busquen causar problemes en el metavers a través de l'assetjament, l'assetjament sexual, la difamació o la violència.

Vàndals

Poden causar danys en el metavers, sigui a través d'atacs DDoS o mitjançant la destrucció de contingut.

Extremistes i terroristes

Poden fer ús del metavers per a difondre la seva propaganda, reclutar nous membres i planificar atacs.

4.4 Tipologia de ciberatacs

S'estima que, en el metavers que està per construir, hi haurà tres ciberatacs especialment preocupants, pel fet que la realitat virtual, per si mateixa, podria facilitar les condicions perquè succeeixin més assíduament.

Les anàlisis de riscos que es realitzin sobre el metavers, hauran de contemplar també les Amenaces Persistents Avançades que puguin donar-se. No obstant això, resulta cada vegada més necessari l'aplicació de mètodes de ciber-intel·ligència per al desenvolupament d'una ciberseguretat més prospectiva.

Denegació de servei distribuït (DDoS)

Aquest tipus de ciberatac col·lapsa el servidor web perquè rep més peticions de servei de les que pot assumir per a mantenir la seva funcionalitat. El metavers suposa una infinitat de nous servidors-objectiu dels quals podran extreure més rèdit que el que obtenen en l'actualitat. Aquests atacs busquen sobrecarregar els servidors del metavers amb sol·licituds no desitjades per a fer-los inaccessibles per als usuaris legítims.

Suplantació d'identitat o *Spoofing*

El metavers podria representar un brou de cultiu per a noves formes de suplantació a causa de l'ús d'avatars, afectant al seu torn altres riscos relacionats, com el *grooming*. Els ciberdelinqüents podrien crear identitats falses en el metavers per a enganyar altres usuaris i obtenir informació personal o financera.

Denegació de servei distribuït (DDoS)

Els atacs de denegació de servei (DDoS) tenen per objectiu interrompre els serveis oferts per llocs web o qualsevol altre recurs de xarxa, sobrecarregant el seu trànsit.

Atacs DDoS

Els atacs de denegació de servei (DDoS) tenen per objectiu interrompre els serveis oferts per llocs web o qualsevol altre recurs de xarxa, sobrecarregant el seu trànsit.

A més dels tipus d'atacs esmentats prèviament, també podrien donar-se els següents atacs:

Ransomware

Els virus segrestadors podrien ser un gran problema en el metavers, on els usuaris custodien béns virtuals de gran valor econòmic, convertint-se així en objectius propicis per a aquest ciberatac.

Phishing

Els ciberdelinqüents podrien crear llocs web falsos o enganyosos en el metavers per a obtenir informació personal o financera dels usuaris.

Malware

Amb el programari maliciós s'infectarien dispositius utilitzats per a accedir al metavers i robar informació personal o financera.
És important tenir en compte que aquests atacs i la forma en què podrien ser executats estan en constant evolució, per la qual cosa és important mantenir-se actualitzat amb les últimes tendències i mesures de seguretat per a protegir-se contra qualsevol ciberatac en el metavers.

5. REPTES I DESAFIAMENTS DE LA SEGURETAT AL METAVERS

La ràpida evolució de les tecnologies relacionades amb el metavers suposa un desafiament per a supervisors, empreses, i usuaris, els qui han d'abordar de manera conjunta aspectes ètics, legals, i tecnològics. No sols ens trobarem amb problemes típics de l'era d'internet, els quals estaven relacionats amb la privacitat, la identitat, les dades i la ciberseguretat dels equips informàtics. Ara amb el metavers sorgeixen noves qüestions que, segons hem explicat, tenen a veure amb la seguretat de les transaccions basada en les criptomonedes, NFT's i actius en el metavers.

A continuació, explicarem els reptes i desafiaments de la Ciberseguretat en el metavers:

Regulació

Com ja s'ha esmentat, un dels aspectes claus per a garantir la ciberseguretat en el metavers és la regulació. Encara no existeixen encaixos jurídics o recomanacions públiques sobre aquests nous entorns immersius en línia, els quals incorporaran noves tecnologies de realitat virtual i augmentada amb els desafiaments que això comporta.

Identitat i privacitat

Els avatars són la nova identitat digital dels usuaris en el metavers, per la qual cosa serà necessari establir protocols de seguretat per a evitar falsificacions, hackejos i poder identificar amb seguretat a l'avatar amb el qual s'interactua. Això té especial rellevància si l'ús del metavers es desenvolupa en sectors sensibles com la medicina i els serveis financers.

Plataformes

La relació i interoperabilitat entre plataformes i serveis sempre suposa un repte en termes de competència. Però també la relació entre les plataformes i els usuaris, que hauran de gestionar els drets de propietat intel·lectual, els accessos, la identitat, la privacitat, la gestió de les dades, i fins i tot les transaccions financeres.

Moderació i accessos

L'adquisició de terrenys i parcel·les virtuals, la seva propietat, i l'accés a aquests llocs plantejaran nombrosos dilemes sobre les responsabilitats de l'ús que es realitza a l'interior d'aquests. Si es produeix frau, assetjament o altres formes d'abús, caldria determinar qui o qui són els responsables.

Realitat virtual, augmentada i estesa (VR, AR, XR)

Amb la integració de les noves tecnologies VR/AR/XR en el metavers, els usuaris disposaran d'un major de dispositius amb els quals submergir-se en aquests ecosistemes virtuals. Les ulleres de Realitat Virtual (RV), complements hàptics com a guants i armilles, i un altre tipus de sensors IoT incorporen càmeres i micròfons per al seu funcionament, per la qual cosa aquests dispositius tindran accés a llocs íntims i privats en cases i oficines.

Dades

A causa d'aquesta naturalesa més immersiva d'aquesta tecnologia, la gran quantitat de dades personals que es poden recopilar serà enorme. En comparació amb les xarxes socials, les plataformes de metavers poden recopilar detalls molt més íntims sobre els usuaris. Sense una normativa clara, la protecció o l'intercanvi d'aquestes dades queda completament a discreció del propietari de la plataforma, que comptarà amb informació extremadament valuosa per a comercialitzar sobre el comportament dels usuaris.

Publicitat

A més d'anuncis, tanques publicitàries i promocions en *showrooms*, el metavers també presenta uns certs dilemes i problemes per a limitar els anuncis més comercials. Igual que en les xarxes socials, qualsevol avatar es pot convertir en un ambaixador d'una marca, desdibuixant les línies en el contingut real i el promocional.

Treball

El metavers portarà amb si la generació de nous llocs de treball i s'estima que els equips serien més multidisciplinaris, més eficients i amb una major productivitat en la consecució de les tasques i consecució d'objectius.

6. RECOMANACIONS

És important desenvolupar una mentalitat de seguretat i privacitat de base, ja que el nombre d'interaccions i la proliferació de dades en el metavers han de protegir-se adequadament. A més, els algorismes que impulsen les experiències del metavers estan en constant desenvolupament, la qual cosa crea una complexitat addicional que haurà de ser revisada, monitorada i protegida. La tasca de protegir els actius, les dades i les persones és enorme i haurà de ser compartida per aquells que treballen en el metavers i els usuaris, així com pels organismes governamentals que proporcionen regulació sobre el flux de dades entre ells.

Implementar protocols

Les empreses de metavers haurien d'implementar protocols d'encriptació i autenticació per a protegir la informació personal i les dades delicades, així com el monitoratge de sistemes i xarxes per a detectar i prevenir atacs cibernètics.

Formació als empleats

Les empreses que construeixen amb Web 3.0 han d'assegurar-se que els seus empleats tinguin les habilitats i eines per a identificar amenaces internes i externes, així com prendre les mesures adequades per a reduir els riscos de seguretat. En el passat, moltes empreses van perdre la confiança del consumidor a causa de la falta de seguretat i pràctiques segures en les aplicacions Web 2.0. Tots els empleats han d'estar formats i equipats amb la informació correcta per a ajudar a garantir la seguretat personal i empresarial i evitar la proliferació de dades i bretxes. Internament, les organitzacions

necessiten implementar un enfocament educatiu i la creació de paradigmes d'interacció en un metavers.

Formació/sensibilització a usuaris

És important educar als usuaris sobre els riscs potencials associats amb el metavers i encoratjar-los a prendre mesures per a protegir-se a si mateixos i la seva informació personal.

Protecció de privacitat en línia

Per a protegir-nos com a usuaris podem usar eines de seguretat. Per exemple, comprar un *proxy* i emprar-ho per accedir al metavers. Un *proxy* d'alta velocitat permetrà ingressar al metavers de manera anònima, ocultant l'IP real als ciberdelinqüents.

Regulació i governança

Un sistema de regulació i governança amb intermediaris reconeguts és essencial per a garantir la supervisió del metavers i generar confiança. Per exemple, les transaccions financeres realitzades a través d'avatars intel·ligents generaran dades, per la qual cosa sorgeixen preguntes sobre com han de processar-se i regular-se aquestes dades i quins contractes han d'existir per a garantir la privacitat.

7. GLOSSARI

Amenaça Persistent Avançada

Una amenaça persistent avançada, també coneguda per les seves sigles en anglès, APT (per *Advanced Persistent Threat*), és un conjunt de processos informàtics sigil·losos orquestrats per un tercer (organització, grup delictiu, una empresa, un estat, etc.) amb la intenció i la capacitat d'atacar de forma avançada (a través de múltiples vectors d'atac) i continuada en el temps, un objectiu determinat (empresa competidora, estat, etc.).

Atac Sybil

En seguretat informàtica, un atac Sybil ocorre quan un sistema distribuït és corromput per una mateixa entitat que controla diferents identitats d'aquesta xarxa.

Avatar

És un personatge tridimensional personalitzat que s'ha de crear per a accedir al metavers i que és la interfície a través de la qual interactuaràs amb la resta de persones d'aquest.

Big data

El Big Data són el conjunt de tecnologies que han estat creades per recopilar, analitzar i gestionar les dades que generen els usuaris d'Internet. La seva idea és la d'ajuntar les dades massives que s'han generat en "brut", i processar-les per identificar patrons o un altre tipus de comportaments que puguin ajudar a sectors concrets.

Blockchain

El *blockchain* (també conegut com «el protocol de la confiança») és una tecnologia que apunta a la descentralització com a mesura de seguretat. Es tracta de bases de registres i dades distribuïdes i compartides amb la funció de crear un índex global per a totes les transaccions que es generen en un determinat mercat. Funciona de manera pública, compartida i universal, ja que crea consens i confiança en la comunicació directa entre ambdues parts, és a dir, sense l'intermedi de tercers.

Ciberatac

Intent deliberat d'un ciberdelinqüent d'obtenir accés a un sistema informàtic sense autorització servint-se de diferents tècniques i vulnerabilitats per la realització d'activitats amb finalitats malicioses, com ara el robatori d'informació, extorsió del propietari o simplement danys al sistema.

Grooming

El *grooming* és una manera d'assetjament que suposa el contacte d'un adult amb un menor per guanyar-se la seva confiança a poc a poc i posteriorment implicar-lo en alguna actuació de caràcter sexual. Les actuacions poden anar des de demanar al menor l'enviament de contingut íntim a arribar a tenir trobades sexuals.

Enginyeria Social

Pràctica per obtenir informació confidencial a través de la manipulació d'usuaris legítims. És una tècnica que poden usar unes certes persones per aconseguir informació, accés o permisos en sistemes d'informació que els permetin realitzar danys a la persona o organisme compromesos. El principi que sustenta l'enginyeria social és el que, en qualsevol sistema, els usuaris són l'«esgraó feble».

Intel·ligència Artificial (IA)

La intel·ligència artificial és l'habilitat d'una màquina de presentar les mateixes capacitats que els éssers humans, com ara el raonament, l'aprenentatge, la creativitat i la capacitat de planejar.

Internet de les coses (IoT)

Aquest concepte descriu objectes físics amb sensors, capacitat de processament, programari o altres capacitats tecnològiques que faciliten, mitjançant internet, la comunicació entre dispositius i/o sistemes.

Malware

És un tipus de programari que té com a objectiu danyar o infiltrar-se sense el consentiment del seu propietari en un sistema d'informació. El mot neix de la unió dels termes en anglès de programari maliciós: *malicious software*. Dins d'aquesta definició té cabuda un ampli ventall de programes maliciosos: virus, cucs, troians, *backdoors*,

spyware, etc. La part que comparteixen tots aquests programes és el seu caràcter nociu o lesiu.

Non-fungible tokens (NFT)

Un token no fungible és un actiu digital encriptat. Es tracta d'un tipus especial de token criptogràfic que representa una cosa única. Els tókenes no fungibles no són, per tant, intercanviables de manera idèntica.

Ransomware

Programari maliciós mitjançant el qual els atacants aconsegueixen xifrar la informació continguda en un sistema després de comprometre'l. En general, s'utilitza amb l'objectiu de sol·licitar una quantia econòmica a la víctima.

Realitat augmentada

És una realitat mixta, consisteix en la inclusió de mitjans audiovisuals 3D en el món material. La seva relació amb la tecnologia hologràfica ens permetrà observar objectes virtuals en 3D i canviar l'aparença d'objectes que existeixen en el món material, modificant els seus colors i formes.

Realitat virtual

És un món compost per elements virtuals. Es tracta d'una realitat alternativa on podrem desenvolupar relacions, comerços, comunitats i activitats juntament amb altres persones, així com crear entorns i objectes que en el món material són impossibles.

Tecnologies de la informació (TI o IT)

Eines i aplicacions amb les quals es dota a ordinadors i equips de telecomunicacions amb la capacitat d'emmagatzemar, recuperar, transmetre i manipular dades.

Troià

Programari maliciós que es fa passar per programari legítim amb l'objectiu d'enganyar usuaris i sistemes per infectar-los i comprometre'ls.

CLÀUSULA DE CONFIDENCIALITAT