Newsletter
Centro de Investigaciones y Estudios Estratégicos
ANEPE

Editorial

"La dimensión del Metaverso: entre ficción y realidad"

Fuente: MCARDLE, Jennifer and DOHRMAN, Caitlin. The full potencial of a military metaverse. War on the rocks, 18 de febrero 2022. [en línea] [fecha de consulta 1 de agosto 2022] Disponible en: https://warontherocks.com/2022/02/the-full-potential-of-a-military-metaverse/

Fuente: DAY, Joe. Metacerse will see cyberwarfare attacks unlike anything before: "massivley elevated". Express, 28 de febrero de 2022. Imagen: GETTY. [en línea] [fecha de consulta 1 de agosto 2022] Disponible en: https://www.express.co.uk/news/science/1570844/metaverse-news-cyber-warfare-attacks-virtual-worlds-russia-china-spt

Metaverso ha comenzado a constituirse como una nueva dimensión sobre la cual la Aldea Global ha volcado su atención. En palabras simples, el Metaverso trata de una exposición espacial y sensorial que puede entregar una realidad alternativa a la que comúnmente conocemos. Esta realidad alternativa surgió en la década de los noventa, sin embargo su concepción data de mucho antes. Neal Stephenson describió en sus libros de ciencia ficción una dinámica que unió el concepto meta al universo, dando como resultado esta nueva realidad.

Tras la explosión del internet, en la década de los noventa, se vio nacer a los avatares, considerados como la primera ola de realidad virtual. Rápidamente se transitó a la tercera ola, conocida como la realidad del Metaverso un ambiente que se potencia con la Web3, el blockchain, así como los Not Fundgibles Tokens (NFT).

Uno de los principales impulsores de esta nueva dimensión es Mark Zuckerberg, creador de Facebook, y que cambió el nombre de la empresa por Meta, pretendiendo relacionarla con nuevas tecnologías disruptivas. Ya no solo ha comenzado a invertir grandes sumas de dinero, sino que también en capital humano. Sin embargo, los costos del desarrollo e implementación no se han traducido en mayores inversiones.

Por otra parte, un área en donde el metaverso aún pareciera un misterio es en la industria de la Defensa. Recientes estudios de la Fuerza Aérea de EE. UU., han determinado que en China se están preparando para la próxima etapa, postulando que la guerra del Metaverso se posicionará como el escenario más importante. Esta nueva realidad no solo requerirá que los soldados estén físicamente entrenados, sino además deberán poseer capacidades y competencias tecnológicas.

Esta condición virtual permitiría reducir las bajas en el combate real, del mismo modo podrían desaparecer los heridos y/o fallecidos. Una realidad no tan lejana que de avanzar en su desarrollo, está cada vez más cerca. Esta carrera la lidera China y Estados Unidos, y cómo no, las dos potencias que continuamente compiten por alcanzar el sitial de poder e influencia a nivel mundial.

El CIEE, tomando en consideración los alcances y repercusiones que puede acercar el Metaverso, considera relevante presentar los antecedentes que han sido difundidos, para así contribuir a un debate que no se ha dado, principalmente porque no solo se relaciona con ámbitos tecnológicos, económicos y estratégicos, sino que además puede afectar a la sociedad de un mundo globalizado.

CIEE-ANEPE

Los artículos seleccionados para este Newsletter, tienen relación con el desarrollo tecnológico, económico y de Seguridad y Defensa.

Dentro de una nueva carrera militar para dominar el metaverso mientras Estados Unidos y China se preparan para la guerra cibernética

Christopher Eberhart

The Sun, 19 de abril 2022

El metaverso aún está en pañales, pero su potencial ilimitado está seduciendo a las empresas para que inviertan miles de millones de dólares en su desarrollo. La mayoría de los usos potenciales en los EE. UU. se han relacionado con fines civiles comerciales y recreativos. Pero China se está preparando para una guerra de metaverso que "afecta el pensamiento, la cognición y la toma de decisiones de acción del oponente", según un informe de marzo de 2022 de un grupo de expertos de la Fuerza Aérea.

Elmer Francisco, director ejecutivo de la Fundación VetCoin, le dijo a The Sun que el metaverso es el próximo paso evolutivo en armamento después de los drones. "Antes, la gente usaba espadas para pelear. Luego pistolas y otras armas. Ahora, los países usan drones. Es similar, excepto que ahora en el metaverso, los soldados usan computadoras para participar en la guerra cibernética", dijo Francisco. "Los soldados no solo necesitarán saber cómo realizar un combate cuerpo a cuerpo, sino también cómo codificar. Los soldados requieren manipular el dominio virtual". […]

La excepción sería XR, realidad extendida, tecnología que "usarías para manipular el mundo real con máquinas aunque no estés allí físicamente", dijo. "En el ejército, no habrá soldados que necesiten ser amputados porque sería su robot el que explotaría con explosivos", dijo Francisco. "Sería como un juego de computadora. Simplemente aparecerás en otro lugar. Habría una base donde estarían estos robots o avatares y algún soldado de los Estados Unidos controlando ese robot".

[…] "Cuando tienes la tecnología más avanzada, que durante mucho tiempo después de la Guerra Fría, Estados Unidos posee la tecnología más avanzada en términos de muchas cosas, especialmente en lo militar. Es por eso que otros no se meten con Estados Unidos antes. "Ahora lo hacen porque el campo de juego se ha nivelado. Por eso Rusia y China se apresuran a desarrollar su propia tecnología", dijo Francisco.

En teoría, cuanto más fuerte sea el elemento de disuasión, más se puede utilizar esta tecnología con fines humanitarios, como misiones médicas, en lugar de conflictos violentos. "Esa tecnología depende de cómo la uses", dijo. "Puedes usar tu teléfono celular para llamar a un ser querido o puedes usarlo para detonar una bomba. "Es muy importante lograr que la tecnología sea lo más avanzada posible para que nadie piense siquiera en hacer algo tonto como una guerra".

China se prepara para la "guerra del metaverso"

El informe, publicado por el Instituto de Estudios Aeroespaciales de la Fuerza Aérea de China, cita a autores chinos del instituto de investigación de más alto nivel del Ejército Popular de Liberación (EPL) de China. En este momento se desconoce cómo será exactamente la "guerra del metaverso". Pero los autores chinos proporcionan tres estilos de confrontación: "confrontación de plataforma, ataque al sistema (cadena de suministro) y desviación indirecta", según el informe del grupo de expertos de la Fuerza Aérea.

La confrontación de plataformas se describe en el informe como ataques "para interrumpir, retrasar, disuadir, destruir y eliminar la existencia y el funcionamiento del metaverso del oponente". El ataque al sistema "atacará y bloqueará los nodos clave y las cadenas de operaciones tecnológicas que respaldan el metaverso de un adversario". Y la desviación indirecta puede "perjudicar los dispositivos de tecnología de comunicación y usar medios engañosos para alterar la funcionalidad del sistema de metaverso de un adversario".

¿Quién está ganando la 'carrera tecnológica´?

Con mega corporaciones como Meta (anteriormente Facebook) con sede en EE. UU. y varios gigantes tecnológicos de Silicon Valley que invierten tanto dinero en el metaverso, Francisco dijo que cree que EE. UU. está liderando el camino. "Durante muchas, muchas décadas, Estados Unidos siempre ha estado a la vanguardia en el mundo virtual y el espacio", dijo. […]

El informe del grupo de expertos de la Fuerza Aérea, que cita una publicación china titulada "¿Quién puede ganar el metaverso?" - dijo que Estados Unidos está "muy por delante en el metaverso".

[…] "En otro artículo, 'New Battlefield–Metaverse', el autor ubica el metaverso como una extensión de la gran competencia de poder entre Estados Unidos y China", según el informe del grupo de expertos de la Fuerza Aérea. "El autor escribe: 'En el futuro, China y Estados Unidos inevitablemente competirán en el metaverso'.

"El metaverso, aunque todavía está en su infancia, se convertirá en un reflejo de la sociedad real en el futuro y las cuestiones de jurisdicción serán una de las muchas áreas de conflicto entre las dos naciones".

EBERHART, Christopher. Dentro de una nueva carrera militar para dominar el metaverso mientras Estados Unidos y China se preparan para la guerra cibernética. The Sun, 19 de abril 2022.[en línea]. [fecha de consulta 15 de julio 2022] Disponible en: https://www.thesun.co.uk/news/18311412/metaverse-military-race-war-us-china/

El metaverso podría avaluarse en $5 billones de dólares para 2030

Semana

12 de julio 2022

El Metaverso hace parte de las revoluciones tecnológicas que han surgido de las grandes compañías de este mundo, como Facebook y Microsoft. Actualmente, invertir en su desarrollo se perfila como la mayor oportunidad de crecimiento para varios sectores en la próxima década, dada la gran amplitud de aplicaciones, usos potenciales y el grado de inversión.

Es por esto que, los expertos de McKinsey, una compañía especializada en asuntos globales, esperan que el valor económico del metaverso aumente exponencialmente, impulsado por factores como su capacidad para integrar diversos tipos de personas alrededor del mundo, la disposición de los consumidores para gastar en activos digitales, la fuerte inversión empresarial y la retroalimentación positiva que están recibiendo las marcas que ya experimentan este mundo.

Su crecimiento es tal, que las grandes empresas de tecnología, capital de riesgo, capital privado, nuevas empresas y marcas establecidas buscan capitalizar la oportunidad en este espacio a través de la construcción de plataformas digitales patentadas, proporcionando productos y servicios a los usuarios o construyendo hardware y software. Como el caso de Meta, que invirtió más de 10.000 millones de dólares en su división Reality Labs 20 para fabricación de hardware relacionado con el metaverso (como las gafas de Realidad Virtual) y Microsoft adquirió la compañía de juegos Activision Blizzard, que proporcionaría los bloques de construcción para este espacio.

Eric Hazan, socio senior de McKinsey & Company, comenta que "el metaverso representa un punto de inflexión estratégico para las empresas y presenta una oportunidad importante para influir en la forma en que vivimos, nos conectamos, aprendemos, innovamos y colaboramos". Para incursionar en este espacio, Hazan propone tres fases:

La primera se basa en el desarrollo de una estrategia enfocada en el valor que defina metas específicas y el rol que se quiere asumir como empresa dentro del metaverso; la segunda es un intento por probar, aprender y adoptar esta tecnología. En este caso se aconseja experimentar con actividades y casos iniciales para monitorear los resultados a corto plazo y así identificar las métricas adecuadas para conocer

a los usuarios y sus necesidades; y finalmente, prepararse para crecer de diversas maneras, especialmente contratando talento especializado en infraestructura y herramientas tecnológicas, e integrar el metaverso en su estrategia de negocio y modelo operativo.

SEMANA. El metaverso podría avaluarse en $5 billones de dólares para 2030. Semana, Tecnología, 12 de julio 2022. [en línea][fecha de consulta 15 de julio 2022] Disponible en: https://www.semana.com/economia/capsulas/articulo/el-metaverso-podria-avaluarse-en-5-billones-de-dolares-para-2030/202207/

Cómo garantizar la seguridad en un mundo de amenazas híbridas

Miquel Echarri

El País, 20 de junio 2022

En 2005, dos militares estadounidenses, Frank Hoffman y James Mattis, participaron en un proyecto de investigación del Pentágono sobre el carácter cambiante de los conflictos contemporáneos. De ahí surgió un informe hoy pionero, Conflict in the 21st Century: The Rise of Hybrid Wars (Los conflictos en el siglo XXI: El auge de las guerras híbridas), publicado en 2007. En él se hablaba por vez primera del concepto de amenazas híbridas, en el sentido que damos a la expresión en la actualidad, es decir, como los medios no convencionales de agresión que permiten a un enemigo desestabilizar y causar daño sin hacer uso de un ejército regular ni poner un pie sobre el terreno.

Siguiendo a otro investigador militar, Nathan Freier, el informe se refería ya a actos hostiles "irregulares" como campañas de desinformación, propaganda y acciones de descrédito y, muy especialmente, ataques tecnológicos disruptivos (ciber-operaciones, uso de biotecnología, inteligencia artificial o nanotecnología…). Su conclusión era que Estados Unidos y las democracias occidentales en general debían desarrollar y refinar sus herramientas de respuestas contra este tipo de agresiones no bélicas perpetradas por actores no gubernamentales como grupos terroristas o por regímenes autoritarios como Rusia, China, Irán o Corea del Norte.

La era de la gran incertidumbre

El concepto ha hecho fortuna porque describe muy bien el nuevo contexto global en que nos movemos. Aunque la guerra de Ucrania nos ha recordado que una agresión militar convencional sigue sin ser un escenario en absoluto descartable, en los 15 años transcurridos desde que Hoffman y Mattis dieron a conocer su trabajo, las amenazas irregulares y difusas se han multiplicado. Rubén Arcos, docente e investigador de la Universidad Rey Juan Carlos y miembro del comité de expertos del Centro Europeo de Excelencia para Combatir las Amenazas Híbridas (Hybrid CoE) de Helsinki, habla de un muy amplio espectro de "actividades maliciosas con potencial desestabilizador".

[…] Arcos considera que todas las amenazas híbridas parten de un mismo principio, "identificar vulnerabilidades en las sociedades atacadas y explotarlas de manera oportunista". El experto habla de 13 dominios, "de la diplomacia a la economía pasando por las infraestructuras, el prestigio de las instituciones o la imagen de marca de las empresas nacionales" en las que un estado puede ser vulnerable. "Se trata de un espectro ambiguo entre la paz y la guerra en el que la agresión externa puede consistir, por ejemplo, en una campaña de descrédito contra la Unión Europea orquestada en las redes sociales, el hackeo de las infraestructuras digitales, los bulos y demás estrategias de desinformación, acciones contra aeropuertos o la estructura hotelera…". En los últimos años, cobran protagonismo las amenazas híbridas de base tecnológica, "basadas en explotar el alto grado de digitalización e interconexión de nuestras empresas o instituciones", y aparecen nuevas vulnerabilidades "en los mercados de criptoactivos, el metaverso, los sistemas de inteligencia artificial o la economía de datos".

La iniciativa del agresor

Para Guillem Colom, profesor de Derecho en la Universidad Pablo de Olavide y autor para el Instituto Español de Estudios Estratégicos (IEEE) del informe Amenaza híbrida: mitos, leyendas y realidades, "el concepto se puso de moda en 2006, durante el conflicto entre Israel y Hezbolá, cuando se hizo evidente que la milicia palestina estaba actuando como agente delegado (proxy) de Irán y que disponía de drones, misiles anticarro… Es decir, gran parte de los sofisticados recursos bélicos de un Estado". De ahí que se hiciese necesario "hablar de un término medio entre conflicto militar convencional y agresiones irregulares y se acabase recurriendo a la expresión guerra híbrida".

El concepto de hibridación hizo fortuna y resultó "ser muy elástico, por lo que hoy se utiliza para casi todo, de manera a veces un poco abusiva". Pese a todo, Colom acepta que sí es cierto que vivimos en un entorno de "amenazas difusas, muchas de ellas con una robusta base tecnológica". […]

Es el viejo dilema de la lanza y el escudo. El agresor tiene una serie de ventajas cualitativas con respecto al defensor. Entre otras cosas, porque sabe cuándo y cómo se producirá el ataque. Guillem Colom reconoce que la constatación de este hecho puede conducir a una cierta "impotencia y melancolía". Pero contra el pesimismo de la razón se puede (y se debe) oponer siempre el optimismo de la voluntad. La defensa siempre puede fortalecerse. Tal y como explica Rubén Arcos, "contra amenazas difusas, sociedades resilientes y robustas". Contra la propaganda interesada y las campañas de descrédito de las instituciones, "transparencia, coherencia y ciudadanos bien informados". Contra el uso disruptivo de la tecnología, "expertos en ciberseguridad que investiguen para crear nuevas capacidades de prevención y respuesta".

Contra riesgos híbridos, seguridad híbrida

La misma lógica de protección innovadora y proactiva puede aplicarse a la seguridad privada, otro ámbito en el que las amenazas convencionales conviven de manera creciente con un nuevo surtido de peligros irregulares y difusos. Fernando Abós, director general de Prosegur Security, una de las compañías líderes de este segmento de mercado, explica que su empresa ha acuñado un nuevo concepto estratégico, "seguridad híbrida", que, partiendo de un análisis de las nuevas tendencias del mundo en que vivimos y los volátiles contextos en que nos movemos, sirve de guía a su modelo de negocio.

Desde Prosegur se han desarrollado y publicado diversos estudios sobre las que consideran que van a ser las claves del futuro inminente. En ellos se reflexiona sobre el previsible incremento del desorden social y auge del crimen organizado. Se analiza la guerra de Ucrania como un ejemplo de riesgo sistémico: es decir, susceptible de generar una cadena de amenazas derivadas (altos niveles de inflación, subida de tipos de interés, migraciones masivas, crisis alimentarias, nuevas primaveras revolucionarias…).

[…] ¿Cómo se hace eso? Con innovación y una sólida base tecnológica. Practicando, como sugería Arcos en el terreno de la geopolítica, un pensamiento creativo y prospectivo que se anticipe a las amenazas y fortalezca las defensas. De ahí que, tal y como explica Abós, Prosegur esté adaptando su modelo de negocio partiendo de una nueva base conceptual: proporcionar a su plantilla de expertos en seguridad todo un arsenal de tecnologías inteligentes y conectadas que aprovechan los datos de manera estratégica.

[…] Los primeros, los vigilantes, aportan la necesaria dosis de "experiencia e inteligencia contextual". Y su eficacia cuenta con el auxilio de la tecnología más innovadora potenciada por un modelo global de datos e inteligencia que permite hacer frente tanto a lo previsible como a lo disruptivo: "Debemos estar preparados, porque el cambio que se está produciendo, es exponencial", explica Abós. "Estamos en un momento en que

hay que extremar la consciencia situacional para poder detectar señales que se conviertan en alertas tempranas. Y, a la vez, entender las tendencias subyacentes que permitan dibujar y revisar escenarios futuros".

[…] Todo muy en la línea de la receta global que promueve el Centro Europeo de Excelencia del que forma parte Rubén Arcos: "No podemos prever todas las amenazas potenciales, pero sí entender mejor qué sucede para potenciar nuestra capacidad de respuesta y reducir nuestras vulnerabilidades". En última instancia, se trata, como señala Colom, "de movernos con inteligencia en un entorno convulso y volátil y encontrar una manera flexible de que prevalezcan nuestros valores y nuestro modelo de sociedad". […]

ECHARRI, Miquel. Cómo garantizar la seguridad en un mundo de amenazas híbrida. El País, 20 de junio 2022. [en línea] [fecha de consulta 15 de julio 2022] Disponible en: https://elpais.com/economia/entorno-seguro/2022-06-20/como-garantizar-la-seguridad-en-un-mundo-de-amenazas-hibridas.html

El sueño del metaverso abierto para todos

Natalia Vera Ramírez

América Económica, 24 de junio 2022

Poco a poco, el metaverso se torna cada vez más real. El número de empresas que invierten millones de dólares para adquirir terrenos virtuales y crear experiencias inmersivas crece día a día. Por su lado, las grandes tecnológicas se han tomado muy en serio las inversiones en este campo alternativo de negocio. Es el caso de Meta (ex Facebook), empresa dirigida por Mark Zuckerberg, que hasta le cambió de nombre por uno bastante ad hoc para estos tiempos de mundos alternativos.

A la par de las sucesivas inversiones en este campo virtual, la proliferación de plataformas y empresas con sus propios metaversos planteaban la pregunta sobre la interoperabilidad entre ellas. Y es que en el futuro -cada vez más cercano- los usuarios no se van a limitar a un solo metaverso.

Una posible salida a este dilema se dio el esta semana, cuando Meta, Microsoft y otros gigantes tecnológicos anunciaron la creación de Metaverse Standards Forum, un grupo para fomentar el desarrollo de estándares de la industria que harían que los mundos digitales nacientes de las empresas sean compatibles entre sí.

El objetivo es ofrecer una mejor experiencia a los usuarios que, validos de lentes de realidad virtual o aumentada, puedan transitar de un metaverso a otro sin turbulencias en el camino, al tener plataformas abiertas en las que se puedan usar todas las herramientas para el metaverso creadas por las compañías que están compitiendo en esta carrera.

A esta iniciativa se han unido compañías muy variopintas que van desde fabricantes de chips, compañías de juegos, empresas de redes y de dispositivos de realidad virtual y aumentada hasta firmas de retail como Ikea y asociaciones como el World Wide Web Consortium (W3C), según informó el grupo en un comunicado.

El gran ausente en este flamante grupo es Apple, que aún no confirma públicamente el lanzamiento de un auricular de realidad mixta. No obstante, los analistas estiman que una vez que esto se concrete, la empresa de Steve Jobs se convertirá en un jugador dominante en la carrera del metaverso y en un fuerte competidor para Meta que ha hecho de este mundo virtual su caballito de batalla en los últimos meses.

Incluso, Meta ya ha compartido algunos avances de sus futuros visores y todo indica que presentará nuevas gafas antes de que termine 2022. La ocasión para este lanzamiento podría ser el próximo Meta Connect de la compañía.

Otros jugadores tecnológicos que no han participado de este grupo son las empresas de juegos Roblox y Niantic. Tampoco The Sandbox, uno de los principales metaversos cripto y Decentraland.

Más allá de quiénes formen parte de este grupo y mantengan abiertas las fronteras del metaverso, lo cierto es que la carrera de quién lo liderará ya arrancó. Si bien algunos especialistas afirman que esto no implica que las empresas crearán "el metaverso" como un espacio interconectado, al mismo estilo de la World Wide Web (www), de hecho si es un gran paso para facilitar que los desarrolladores creen el mismo contenido para diferentes plataformas o que los usuarios exporten datos de un servicio a otro.

VERA Ramírez, Natalia. El sueño del metaverso abierto para todos. América Económica, 24 de junio 2022. [en línea] [fecha de consulta 22 de julio 2022] Disponible en: https://www.americaeconomia.com/metaverso-abierto-para-todos

La entrada desprotegida en el metaverso trae riesgos cibernéticos acumulados

Zawya

22 de julio 2022

Las empresas que están considerando unirse al carro del metaverso han sido puestas en alerta máxima contra ataques cibernéticos inminentes que podrían exponer sus datos valiosos a ataques cibernéticos paralizantes, exfiltración de datos e infracciones.

A medida que las marcas se sumergen cada vez más en el metaverso, impulsadas en gran medida por las emocionantes oportunidades que presenta este concepto digital relativamente nuevo, los expertos en ciberseguridad y TI están seriamente preocupados porque la mayoría de ellos se apresuran a establecer su presencia sin una estrategia de ciberseguridad adecuada.

Metaverso, un intento de crear un mundo virtual inmersivo que combina realidad aumentada y virtual, incluye espacios económicos y sociales donde los usuarios de cualquier parte del mundo pueden disfrutar de una amplia gama de contenidos y experiencias.

Esto, según los expertos en ciberseguridad, también expone significativamente a los usuarios individuales de Internet y las marcas que juegan en ese espacio a una gran cantidad de riesgos que podrían provocar un aumento en los casos de piratería y manipulación de cuentas, phishing y robo de activos.

"Metaverso es un concepto emocionante y futurista que está creando enormes oportunidades tanto para las empresas como para los innovadores. Sin embargo, las empresas que están considerando operar en ese espacio también deben tener cuidado con las amenazas cibernéticas inminentes que vienen con las nuevas innovaciones. Tan pronto como la propiedad digital en el universo 3D, por ejemplo, adquiera valor, los casos de piratería de cuentas, robo, ransomware y phishing también aumentarán significativamente. En parte, la culpa será la falta de una estrategia sólida de protección cibernética para salvaguardar la información privada y confidencial de posibles atacantes", dijo Candid Wüest, vicepresidente de investigación de protección cibernética de Acronis.

Según el Informe global de la semana de la ciberprotección de Acronis de 2022, los ciberdelincuentes están explotando la complejidad de TI para lanzar ciberataques catastróficos. Dado que la mayoría de los usuarios aún no son plenamente conscientes de la magnitud de las ciberamenazas a las que se enfrentan a raíz de una mayor adopción del metaverso, es probable que el robo diario de datos (tarjeta de crédito, identidad, contraseñas, etc.), el malware y los ataques de phishing aumenten en 200 % para 2024 debido a la falta de preparación o falta de un plan maestro de protección cibernética.

Principales riesgos

La seguridad de los dispositivos sigue ocupando un lugar destacado en la lista de prioridades de protección cibernética, ya que se espera que la piratería de plataformas y dispositivos aumente a medida que la aceptación del metaverso también se dispara. Es probable que las amenazas y

las infracciones a los dispositivos empeoren y, posteriormente, también podrían tener consecuencias terminales reales en el mundo físico.

"Para los usuarios individuales de Metaverso, la piratería de dispositivos habilitados para Metaverso, como auriculares específicos, por ejemplo, puede causar convulsiones, si alguien es epiléptico. También puede dañar su visión o su audición al menos temporalmente, así como exponer su ubicación física y más", señaló Candid Wüest.

Metaverso no tendrá problemas de seguridad completamente nuevos, ya que tendrá problemas similares a los de la industria del juego. La explosiva popularidad de los juegos, que posiblemente sea el segmento más grande de la industria del entretenimiento, con más de tres mil millones de participantes regulares, pinta una imagen de cuán lucrativo puede llegar a ser el metaverso para los ciberdelincuentes en función de la cantidad de usuarios que puede atraer.

Regulación de datos

La falta de regulación de recopilación y uso de datos también ha surgido como un posible habilitador de amenazas cibernéticas dentro de la plataforma de realidad virtual. Esto, advierten los expertos en seguridad de TI, podría crear una gran cantidad de lagunas que los ciberdelincuentes podrían aprovechar para infiltrarse en redes privadas y obtener acceso sin restricciones a datos confidenciales de empresas e individuos.

Con la falta de regulación, el delito cibernético podría convertirse en el tipo de delito de más rápido crecimiento actualmente valorado en US $ 1-2 billones y creciendo a un ritmo más rápido. Sin embargo, a pesar del compromiso del gigante de las redes sociales Meta de invertir 50 millones de dólares estadounidenses en investigación externa que se centrará principalmente en la privacidad y la seguridad en el metaverso, incluida una asociación con la Universidad Nacional de Singapur para investigar el uso de datos, aún se necesita más. por hacer, especialmente por parte de las empresas para proteger sus datos.

Estas medidas de salvaguarda incluyen una estrategia integral de protección cibernética impulsada por inteligencia artificial y aprendizaje automático combinada con evaluación de vulnerabilidades y pruebas de penetración. Otras medidas de seguridad efectivas incluyen la tecnología blockchain para identificar a los usuarios; tokens asignados por una organización y el uso de datos biométricos en un auricular para confirmar la identidad del usuario.

Guerra del metaverso

Si bien el concepto de un mundo virtual se desarrolló principalmente para las plataformas sociales para ayudarlas a impulsar el compromiso, la multidimensionalidad inmersiva también creará más oportunidades para ataques cibernéticos complejos.

"El Metaverso para la guerra de la información está emergiendo ahora como una amenaza real que podría usarse para difundir información maliciosa. Los problemas como las noticias falsas profundas serán más convincentes en el metaverso, la cobertura de noticias se volverá más "espantosa" y los deportes y el entretenimiento se sentirán más reales. Las emociones se dispararán, lo que en teoría es una debilidad utilizada por los actores de amenazas, incluidos los motivados políticamente", señaló Candid Wüest.

ZAWYA. La entrada desprotegida en el metaverso trae riesgos cibernéticos acumulados. Zawya, 22 de julio 2022. [en línea] [fecha de consulta 23 de julio 2022] Disponible en: https://www.zawya.com/en/press-release/companies-news/unprotected-entry-into-the-metaverse-brings-accrued-cyber-risks-s1h6wugu

Antes de imprimir este Newsletter, piense en el medio ambiente.