وزارت ارتباطات و فناوری اطلاعات
پژوهشگاه ارتباطات و فناوری اطلاعات

راهکارهای مواجه با چالش‌های امنیتی متاورس

تاریخ انتشار

عنوان گزارش: راهکارهای مواجه با چالش های امنیتی متاورس
کلمات کلیدی: امنیت، متاورس
تهیه کنندگان: ساسان کرمی‌زاده، ابوذر عرب‌سرخی
ناظر علمی: امیر منصور یادگاری
گروه پژوهشی: گروه ارزیابی امنیت شبکه و سامانه‌ها
تاریخ نشر: ۱۴۰۳

چکیده

از مفهوم متاورس[۱] برای توصیف دنیای مجازی استفاده می‌شود که در آن کاربران می‌توانند در یک محیط شبیه سازی شده، فعال بوده و با یکدیگر تعامل داشته باشند.

درواقع متاورس با الگوبرداری از دنیای واقعی، یک فضای مشترک دیجیتالی خلق کرده است که در این فضا افراد می‌توانند هم با یکدیگر و هم با اشیا تعامل داشته باشند. محیط متاورس به دلیل اینکه دارای پیوستگی‌های[۲] بسیاری است، با چالش‌های امنیتی سایبری زیادی مواجه است. این مفهوم جدید می‌تواند تجربیات استفاده از اینترنت را دچار تحول کند. امّا، هنوز درحد یک مفهوم نظری و تحقق نیافته باقی مانده است. هدف از این گزارش، شناسایی و بررسی چالش‌های کلیدی در امنیت متاورس و تعیین راه‌حل‌های فناوری برای امنیت آن و همچنین ارائه مسائل قانونی و حکومتی متاورس و ... است.

[۱] Metavers

[۲] interconnected

فهرست مطالب

۱ مقدمه

اصطلاح متاورس اولین بار در سال ۱۹۹۲ ابداع شد، امّا جهان متاورس تا به امروز هنوز ناشناخته است. ممکن است دلیل این موضوع این باشد که متاورس هنوز یک نظریه است و پیاده‌سازی آن در مراحل ابتدایی است. هرچند جهان متاورس به عنوان یک سرزمین ناشناخته نیاز به کاوش بیشتری دارد امّا به زودی بخشی اساسی از زندگی روزمره مردم خواهد شد؛ زیرا این یک محیط است که مردم برای کار، بازی و تعامل با دیگران وارد آن می‌شوند. علاوه بر این، توسط بسیاری از دانشمندان به عنوان اینترنت آینده مشخص شده است و اساساً تکامل وب نسخه ۲.۰ را تشکیل می‌دهد.

امروزه پیشرفت فناوری‌های رایانه‌ای بصورت شگفت‌آوری در حال گسترش است. که می‌توان نمود این پیشرفت را در متاورس "یعنی جایی که دنیای مجازی به موازات دنیای واقعی با استفاده از فناوری وب و فناوری بلاکچین درحال اجرا است" مشاهده نمود. دنیای چندبعدی متاورس با استفاده از ابزارهایی همچون چشم‌افزارهای واقعیت مجازی[۱]، کاربران را از جهان واقعی وارد فراجهان می‌کند؛ جایی که فرد هویتی مجازی و مجزا از چیستی فیزیکی‌اش را ارائه می‌دهد.

باوجود اینکه متاورس دارای مزیت‌های زیادی است؛ امّا به دلیل تلاقی با نظم حاکم در دنیای واقعی دارای چالش‌هایی است. از دید حقوقی، شناخت کامل چالش‌ها و پیامدهای مربوطه می‌تواند برای سیاست‌گذاری و تنظیم‌گری دولت در این زمینه براساس شرایط خاص هر جامعه‌ای ضروری باشد.

کلمه متاورس از ترکیب دو کلمه متا[۲] به معنی فراتر [۳] و ورس[۴] مخفف جهان تشکیل شده است و به معنای واقعی یعنی جهانی فراتر از جهان واقعی می باشد. این اصطلاح که امروزه به طور گسترده استفاده می‌شود به دنیای مجازی سه‌بعدی اشاره دارد که واقعی و غیر واقعی در آن همزیستی دارند. بنابراین، متاورس یک شبکه از جهان‌های مجازی است. در این جهان‌ها، مردم قادر خواهند بود کارهای مختلفی مانند کار یا سرگرمی را بصورت تنهایی یا گروهی انجام دهند.

متاورس یک جهان دیجیتالی گسترده است که واقعیت افزوده[۵]، واقعیت مجازی[۶]، و تجربیات دیجیتالی دیگر را در یک محیط واحد و چند وجهی ترکیب می‌کند. این مفهوم به کاربران اجازه می‌دهد تا در زمان واقعی با یکدیگر و یا

---

[۱] Augmented Reality

[۲] Meta

[۳] beyond

[۴] verse

[۵] Augmented Reality

[۶] Virtual Reality

با اشیاء دیجیتال تعامل داشته باشند و تجربه‌ای غنی و جذاب از فضای مجازی ایجاد کنند. متاورس به‌عنوان اینترنت بعدی تصور می‌شود که در آن واقعیت‌های دیجیتال و فیزیکی به طور یکپارچه ادغام می‌شوند.

با پیشرفت متاورس، پرداختن به چالش‌های امنیتی آن اهمیت بیشتری پیدا می‌کند. با توجه به چندوجهی بودن متاورس و ادغام دارایی‌های واقعی، هویت‌های شخصی و تراکنش‌های مالی، پتانسیل تهدیدات سایبری ناشی از آن قابل توجه است. زیرا اطمینان از اتخاذ تدابیر امنیتی قوی در متاورس برای حفاظت از داده‌های کاربران، حفظ اعتماد و ایجاد محیطی امن برای تعامل و تراکنش ضروری است.

۲ ویژگی‌های متاورس

متاورس دارای ویژگی‌های چند فناوری[۱] است. بدین معنا که به مثابه یک نمود اجتماعی نو دارای ویژگی‌های جمع گرایی[۲] و همچنین پدیده ای موازی با دنیای واقعی، از ویژگی فرا فضایی- زمانی[۳] برخوردار است. متاورس تجربه ای همه جانبه بر پایه فناوری واقعیت افزوده ارائه کرده، تصویری آینه ای از دنیای واقعی براساس فناوری دوقلو دیجیتال[۴] ایجاد می‌کند، و یک سامانه اقتصادی مبتنی بر فناوری بلاک چین می‌آفریند. متاورس مرزهای زمان و مکان را درهم می‌شکند و تجربه‌ای باز، آزاد و مسحورکننده به کاربران ارائه می‌کند. در دنیای واقعی رفتار انسان در زمان و فضای فیزیکی صورت می‌گیرد. فضا و زمان سیر طبیعی رفتار انسان را تضمین می‌کند؛ به‌صورتی که نتواند از ویژگی‌های واقعی مکان و زمان منحرف شود. متاورس تنگناهای زمان و فضا را در دنیای واقعی از دو راه برمی‌دارد: نخست، فراتر رفتن از محدودیت‌های زمان، بازگشت به گذشته و رسیدن به آینده؛ دوم، فراتر رفتن از فضای فیزیکی، پیمودن آن و گذار از فضا و زمان در یک دورهٔ زمانی معین. متاورس دارای ویژگی‌های است که در ادامه به بیان آن‌ها پرداخته می‌شود.

- تعامل‌پذیری[۵]: کاربران با استفاده از این ویژگی می‌توانند داده‌ها خود را از یک پلتفرم به پلتفرم دیگر منتقل کرده و آن‌ها را به ارزش تعیین شده توسط بازار آزاد به دیگر کاربران بفروشند.
- عدم تمرکز[۶]: فناوری بلاک‌چین به متاورس کمک می‌کند تا به سمت (وب ۳) حرکت کند. (وب ۳) مبتنی بر ویژگی عدم تمرکز است که به همه کاربران این امکان را می‌دهد دارایی‌های دیجیتال، داده‌های شخصی و هویت خاص خود را داشته باشند.
- ایداری[۷]: این ویژگی متاورس به کاربران این امکان را می‌دهد تا تجربیات خود را چه مجازی و چه افزوده شده، برای هرکسی که به آن دسترسی دارد و تا زمانی که سازنده تصمیم بگیرد، در دسترس و آنلاین باقی نگه دارد.

---

[۱] Multi-Technology
[۲] Sociality
[۳] Hyper Spatiotemporality
[۴] Digital Twin Technology

" دوقلو دیجیتال یک کپی دیجیتال «مجازی» از هر چیزی در دنیای «فیزیکی» است، خواه یک شخص، یک سازمان، یک سیستم یا چیز دیگری باشد. دوقلوهای دیجیتال وظیفه منحصربه‌فرد کمک به بهبود واکنش‌ها یا ارائه پاسخ‌های دیگر به آنچه در زندگی واقعی اتفاق می‌افتد را دارند. "

[۵] Verifiability
[۶] Decentralization
[۷] Persistency

- جامعه - محوری[۱]: متاورس فرصت جمع‌گرایی و گردهم آمدن افراد پیرامون موضوعات گوناگون را با استفاده از این ویژگی فراهم می‌کند.
- خودحاکمیتی- خودفرمانی[۲]: در متاورس به جای یک پلتفرم یا وب‌سایت، فرد، هویت و داده‌های آنلاین خود را کنترل می‌کند. خودفرمانی، این قابلیت را کاربران و سازندگان قدرت می‌دهد تا زندگی خود را در دستان خود بگیرند.

[۱] Community-Driven

[۲] Self-Sovereignty

۳ چالشهای کلیدی امنیتی در متاورس

در این بخش به چالش‌های کلیدی در متاورس پرداخته می‌شود که شامل عدم حفاظت از هویت داده‌ها، تهدیدات پیشرفته سایبری، عدم امنیت فیزیکی و مجازی و فقدان اصلاحات استاندارد است که در ادامه به توضیحات این عبارت‌ها پرداخته می‌شود.

۳-۱ عدم حفاظت از هویت داده

۳-۱-۱سرقت هویت و جعل

در متاورس، هویت‌های کاربران توسط آواتار[۱]های دیجیتال نمایان می‌شود که می‌تواند مورد سرقت و جعل قرار گیرند. حفاظت از این هویت‌ها نیازمند مکانیسم‌های احراز هویت قوی است. احراز هویت چندعاملی[۲] و تأیید بیومتریک می‌توانند به تأمین حفاظت از حساب‌های کاربری از دسترسی غیرمجاز کمک کنند. علاوه بر این، استفاده از توکن‌های امنیتی فیزیکی یا نرم‌افزاری نیز می‌تواند یک لایه حفاظتی اضافی ایجاد کند. پیاده‌سازی پروتکل‌های امنیتی نظیر OAuthو OpenID Connect نیز در کاهش ریسک سرقت هویت مؤثر است.

۳-۱-۲ عدم حفظ حریم خصوصی داده‌ها

از آنجا که متاورس مقادیر زیادی از داده‌های شخصی را تولید و ذخیره می‌کند، آن را به هدفی جذاب برای مجرمان سایبری تبدیل می‌کند. اطمینان از حفظ حریم خصوصی داده‌ها شامل رمزگذاری اطلاعات حساس و اجرای کنترل‌های دسترسی سختگیرانه برای جلوگیری از دسترسی غیرمجاز به داده‌ها و نقض حریم خصوصی است.

این اقدامات باید شامل رمزگذاری در انتقال باشد. استفاده از فناوری‌های جدید مانند پردازش امن داده‌ها نظیر (AES-۲۵۶) و پایگاه داده‌های محرمانه نیز می‌تواند به حفاظت بهتر (Secure Multi-Party Computation) از حریم خصوصی کمک کند.

---

[۱] Avatar

"آواتارها تصاویری هستند که کاربران در اینترنت و به خصوص در تالار گفتگو برای پروفایل خود استفاده می‌کنند. کاربران عموماً از آواتار خود در شبکه‌های اجتماعی، بازی‌های کامپیوتری و فضای مجازی استفاده می‌کنند."

[۲] Multi-factor authentication (MFA)

۳-۲ تهدیدات پیشرفته سایبری

۳-۲-۱ حملات مبتنی بر هوش مصنوعی

مجرمان سایبری به طور فزاینده‌ای از هوش مصنوعی برای انجام حملات پیچیده استفاده می‌کنند. این موضوع شامل طرح‌های فیشینگ مبتنی بر هوش مصنوعی و فناوری جعل عمیق[۱] برای ایجاد تعاملات دیجیتالی قانع‌کننده امّا جعلی است. دفاع در برابر این تهدیدات نیازمند راه‌حل‌های امنیتی مبتنی بر هوش مصنوعی است که می‌توانند ناهنجاری‌ها را در زمان واقعی شناسایی و پاسخ دهند. به‌علاوه، آموزش مستمر کاربران در مورد شناسایی این حملات و استفاده از فیلترهای هوش مصنوعی برای شناسایی محتوای مشکوک نیز ضروری است.

۳-۲-۲ بدافزار و باج‌افزار

زیست بوم پیچیده متاورس از دستگاه‌ها و پلتفرم‌های متصل، آن را در معرض حملات بدافزار و باج‌افزار قرار می‌دهد. اطمینان از حفاظت کامل نقطه انتهایی و به‌روزرسانی‌های امنیتی منظم برای کاهش این خطرات ضروری است. استفاده از نرم‌افزارهای ضد بدافزار و سیستم‌های تشخیص نفوذ[۲] می‌تواند نقش مهمی در مقابله با این تهدیدات ایفا کند. اجرای سیاست‌های مدیریت پچ[۳] و به‌روزرسانی منظم نرم‌افزارها نیز اهمیت بسیاری دارد.

۳-۳ عدم امنیت فیزیکی و مجازی

۳-۳-۱ عدم امنیت دستگاه‌ها

دستگاه‌هایی مانند هدست‌های واقعیت مجازی و سیستم‌های بازخورد لمسی برای تجربه متاورس ضروری هستند، با این وجود چالش‌های امنیتی منحصر به فردی را نیز به همراه دارند. اطمینان از اینکه این دستگاه‌ها از تغییر و دسترسی غیرمجاز محفوظ هستند برای حفاظت از کاربران در فضای مجازی و فیزیکی ضروری است. پیاده‌سازی پروتکل‌های ارتباطی امن مانند WPA۳ برای وای‌فای و استفاده از مکانیزم‌های احراز هویت دستگاه‌ها نیز اهمیت دارد.

.

---

[۱] Deep Fake

[۲] Intrusion Detection system

[۳] Patch Management

۳-۳-۲ پیامدهای واقعی

چندوجهی بودن متاورس به این معناست که اقدامات دیجیتال می‌توانند پیامدهای واقعی داشته باشند. به‌عنوان مثال، دستکاری دستگاه‌های لمسی می‌تواند منجر به آسیب فیزیکی شود. توسعه پروتکل‌هایی برای اطمینان از تعامل ایمن بین دنیای دیجیتال و فیزیکی برای حفاظت از کاربران ضروری است. این پروتکل‌ها باید شامل مکانیسم‌های جلوگیری از دستکاری و تشخیص فوری نفوذ به دستگاه‌ها باشند.

۴ راه‌حل‌های تکنولوژیکی برای امنیت متاورس

۴-۱ مدل امنیتی اعتماد صفر

۴-۱-۱ اصل اعتماد صفر

مدل امنیتی اعتماد صفر بر اصل "هرگز اعتماد نکن، همیشه تأیید کن" بنا شده است. این رویکرد شامل تأیید مداوم هویت کاربران، دستگاه‌ها و درخواست‌های دسترسی است، صرف نظر از اینکه موقعیت آن‌ها در داخل یا خارج از شبکه باشد. این مدل امنیتی، مفهوم "اعتماد پیش‌فرض" را از بین می‌برد و تأکید بر احراز هویت دقیق و مجوزهای دقیق دارد. استفاده از توکن‌های موقت و نظارت پیوسته بر رفتار کاربران نیز بخشی از این رویکرد است.

۴-۱-۲ پیاده‌سازی در متاورس

پیاده‌سازی اعتماد صفر در متاورس نیازمند سیستم‌های مدیریت هویت و دسترسی پیشرفته است که تعاملات کاربران را به طور مداوم، نظارت و احراز هویت می‌کنند. این سیستم‌ها باید بتوانند فعالیت‌های مشکوک را در زمان واقعی تشخیص دهند و اقدامات مناسب را انجام دهند. استفاده از پروتکل‌های امنیتی مانند SAML و OAuth برای احراز هویت یکپارچه و امن در متاورس بسیار مهم است.

۴-۲ هوش مصنوعی

هوش مصنوعی یکی از فناوری‌های کلیدی برای ساخت متاورس است. متاورس به شکل مجازی وجود دارد ولی فناوری هوش مصنوعی می‌تواند شرایط واقعی برای به وجود آمدن آنرا فراهم کند. بدین معنی که فناوری هوش مصنوعی می‌تواند حجم زیادی از داده‌های تولید شده توسط فعالیت‌های کاربران در متاورس را پردازش کند که عمدتاً به عنوان تولید مدل‌های هوش مصنوعی و ایجاد محیط‌های مجازی ظاهر می‌شود. نقشه برداری از حرکات بدن برای طبیعی‌تر کردن تعامل مجازی و واقعی به عنوان مثال ترجمه همزمان صدا؛ و افزایش تعامل و مشارکت کاربران یک نمونه از آن است. علاوه بر این، متاورس به عنوان یک توسعه دیجیتالی از فناوری‌های زیربنایی برای حل مشکلات و الزامات ظاهر می‌شود. این موضوع باعث می‌شود فناوری هوش مصنوعی با تقاضای کاربردی واقعی خود مطابقت داشته باشد و باعث به روز رسانی پیشرفت نوآوری در فناوری هوش مصنوعی و ایجاد زمینه‌های کاربردی جدید توسط آن شود.

۴-۲-۱ شناسایی و پاسخ به تهدیدات

هوش مصنوعی می‌توانند با تجزیه و تحلیل مقادیر زیادی از داده‌ها برای شناسایی الگوهای نشان‌دهنده تهدیدات احتمالی، امنیت را در متاورس افزایش دهند. این ابزارها قادر به تشخیص ناهنجاری‌ها و واکنش خودکار به آن‌ها هستند، که می‌تواند از حملات سایبری در زمان واقعی جلوگیری کند. علاوه بر این، استفاده از شبکه‌های عصبی برای تحلیل رفتارهای پیچیده کاربران نیز می‌تواند به شناسایی تهدیدات کمک کند.

۴-۲-۲ تحلیل رفتاری

الگوریتم‌های هوش مصنوعی می‌توانند رفتار کاربران در متاورس را تجزیه و تحلیل کنند و فعالیت‌های مشکوکی را که ممکن است نشان‌دهنده تهدید امنیتی باشد شناسایی کنند. با درک الگوهای رفتاری نرمال، این سیستم‌ها می‌توانند، به سرعت انحرافاتی را که نیاز به بررسی بیشتر دارند علامت‌گذاری کنند. این سیستم‌ها همچنین می‌توانند برای پیش‌بینی تهدیدات آینده و ارائه راه‌حل‌های پیشگیرانه استفاده شوند.

۴-۳ غیرمتمرکزسازی و بلاک‌چین

۴-۳-۱ مدیریت امن داده‌ها

فناوری‌های غیرمتمرکزسازی مانند بلاک‌چین راه‌حل‌های قدرتمندی برای مدیریت امن داده‌ها در متاورس ارائه می‌دهند. با توزیع داده‌ها در یک شبکه غیرمتمرکز، این فناوری‌ها خطر نقاط مرکزی شکست و دسترسی غیرمجاز را کاهش می‌دهند. بلاک‌چین می‌تواند شفافیت و ردیابی دقیق تراکنش‌ها را تضمین کند که برای امنیت داده‌ها بسیار مهم است.

۴-۳-۲ حفاظت از دارایی‌های دیجیتال

توکن غیر قابل تبادل یک شناسه دیجیتال منحصر به فرد است که در زنجیره بلوکی ثبت می‌شود و قابل کپی برداری یا تقسیم نمی‌باشد. به دلیل ماهیت اصلی آن‌ها، توکن‌های غیر قابل تبادل، گزینه جذابی برای پول‌شویان در انجام کلاه‌برداری‌های مالی فراهم کرده است؛ و آن‌ها براحتی بدون گذاشتن هیچ اثری از خود فرار کرده‌اند. ارزش توکن‌های غیرقابل تبادل عمدتاً توسط میزان علاقه خریدار تعیین می‌شود. بدین مفهوم که جنایتکاران از پول سیاه خود استفاده می‌کنند تا توکن‌های غیر قابل تبادل را خریداری کنند و سپس آن‌ها را به کاربران دیگر بفروشند و بدین ترتیب دارایی‌های غیرقانونی خود را به دارایی‌های قانونی تبدیل می‌کنند. بلاکچین می‌تواند برای حفاظت از دارایی‌های دیجیتال در متاورس، مانند املاک مجازی و توکن‌های غیرقابل تبادل استفاده شود. با ثبت مالکیت و داده‌های تراکنش در یک دفترکل تغییرناپذیر، بلاکچین اصالت و یکپارچگی دارایی‌های دیجیتال را تضمین می‌کند.

۵ مسائل قانونی و حکومتی

۵-۱ حکمرانی جامعه

۵-۱-۱ ایجاد قوانین و دستورالعمل‌ها

حکمرانی موثر در متاورس شامل ایجاد قوانین و دستورالعمل‌ها برای مدیریت رفتار کاربران و اطمینان از محیطی امن است. این موضوع شامل تنظیم پروتکل‌هایی برای حل و فصل اختلافات، گزارش رفتارهای سوءاستفاده‌گرانه و اجرای استانداردهای جامعه می‌شود. قوانین باید شفاف و قابل اجرا باشند و با توجه به تغییرات فناورانه و اجتماعی به روزرسانی شوند.

۵-۱-۲ نقش ناظران

ناظران نقش مهمی در حفظ نظم در متاورس ایفا می‌کنند. آن‌ها مسئول نظارت بر تعاملات کاربران، اجرای قوانین و رسیدگی به تخلفات هستند. پیاده‌سازی ابزارهای نظارت خودکار می‌تواند به مدیریت محیط‌های بزرگ به طور موثر کمک کند. علاوه بر این، ایجاد تیم‌های پاسخگویی سریع برای برخورد با حوادث امنیتی نیز ضروری است.

۵-۲ ملاحظات قانونی و اخلاقی

۵-۲-۱ قوانین حفظ حریم خصوصی داده‌ها

با پیشرفت متاورس، نیاز به رعایت قوانین موجود در حفظ حریم خصوصی داده‌ها مانند مقررات عمومی حفاظت از داده‌ها[۱] و قانون حریم خصوصی مصرف‌کننده کالیفرنیا[۲] وجود خواهد داشت. این قوانین الزامات سختگیرانه‌ای برای حفاظت از داده‌ها و رضایت کاربران دارند که باید در طراحی متاورس گنجانده شوند. تطبیق با این قوانین می‌تواند اعتماد کاربران را جلب کند و خطرات قانونی را کاهش دهد.

---

[۱] The General Data Protection Regulation

[۲] California Consumer Privacy Act

۵-۲-۲ چالش‌های اخلاقی

ملاحظات اخلاقی در متاورس شامل اطمینان از دسترسی منصفانه، جلوگیری از تبعیض و حفاظت از حقوق کاربران است. توسعه دستورالعمل‌ها و چارچوب‌های اخلاقی برای رسیدگی به این مسائل و ایجاد یک محیط دیجیتال فراگیر ضروری است. این موضوع شامل ایجاد پروتکل‌های شفاف برای جمع‌آوری و استفاده از داده‌ها و اطمینان از عدم سوءاستفاده از قدرت در جوامع متاورس می‌شود.

۶ امنیت مالی

به طور طبیعی، جرائم مالی وارد دنیای متاورس شده است. پیامدهای این امر نه تنها برای قربانیان، بلکه در راستای کاهش پیشرفت و نوآوری فنی نیز بسیار جدی است. همانطور که توسط اتحادیه اروپا اعلام شده است، کلاهبرداری، نه تنها گروه‌های جنایتکار را ثروتمند می‌کند، بلکه توسعه‌های بازار دیجیتال را محدود می‌کند و شهروندان را نسبت به خرید آنلاین بیشتر مردد می‌سازد. همانطورکه در فصل۷ بند ۷۱۳/۲۰۱۹ دستورالعمل (اتحادیه اروپا) بیان شده است.

۶-۱ خطرات ارزهای دیجیتال

۶-۱-۱ پول‌شویی

استفاده از ارزهای دیجیتال در متاورس منجر به ایجاد خطرات مرتبط با پول‌شویی می‌شود. بدین صورت که مجرمان می‌توانند از ناشناس بودن تراکنش‌های ارز دیجیتال برای پنهان کردن فعالیت‌های غیرقانونی استفاده کنند. کاربران متاورس قادر خواهند بود تا به صورت مجازی در تعاملات دیدار کرده و بدون هیچ تهدیدی و به طور کاملاً ناشناس معاملاتی خود را انجام دهند، این سطح حریم خصوصی یک تغییر عظیم در مقایسه با رمزگذاری از انتها به انتها[۱] است و سازمان‌های مراقبت از پولشویی را به چالش می‌کشاند. لذا اجرای اقدامات ضد پولشویی[۲] سختگیرانه برای کاهش این خطرات ضروری است.

۶-۱-۲ حملات باج‌افزار

ارزهای دیجیتال می‌توانند برای تسهیل حملات باج‌افزار در متاورس استفاده شوند. اطمینان از اتخاذ تدابیر امنیت سایبری قوی و آموزش کاربران در مورد اجتناب از طرح‌های فیشینگ و لینک‌های مشکوک می‌تواند به جلوگیری از این حملات کمک کند. به‌کارگیری فناوری‌های رمزنگاری قوی و سیستم‌های پشتیبان‌گیری منظم نیز می‌تواند اثرات این حملات را کاهش دهد.

---

[۱] End-to-End

[۲] Anti-Money Laundering

۶-۲ اقدامات ضد پولشویی

۶-۲-۱ نظارت بر تراکنش‌ها

اقدامات ضد پولشویی شامل نظارت مستمر بر تراکنش‌های ارز دیجیتال برای شناسایی و گزارش فعالیت‌های مشکوک است. استفاده از هوش مصنوعی و یادگیری ماشینی می‌تواند اثربخشی نظارت بر تراکنش‌ها را با شناسایی الگوهای غیرعادی که نشان‌دهنده پول‌شویی هستند، افزایش دهد. توسعه الگوریتم‌های تحلیل پیشرفته نیز می‌تواند در شناسایی فعالیت‌های غیرقانونی کمک کند.

۶-۲-۲ تأیید هویت کاربران

تأیید هویت کاربران از طریق پروسه‌های شناسایی مشتری[۱] به جلوگیری از سوءاستفاده از ارزهای دیجیتال در متاورس کمک می‌کند. اطمینان از اینکه کاربران همان کسانی هستند که ادعا می‌کنند، خطر تقلب و جرایم مالی را کاهش می‌دهد. بهینه‌ترین گزینه برای مقابله با مجرمان از طریق بررسی‌های امنیتی دقیق در زمان ورود مشتری است. شرکت‌های متاورس از سرمایه‌گذاری بر روی "مشتری خود را بشناسید" و اقدامات غربالگری است که می‌توانند هویت واقعی کاربران قانونی را تأیید کنند و در عین حال با بازیگران بد مقابله نموده و گزارش تخلفات را به مقامات مربوطه ارائه دهند.

[۱] Know Your Customer

۷ جهت‌گیری‌های آینده و توصیه‌ها

۷-۱ استراتژی‌های امنیتی پیشگیرانه

۷-۱-۱ممیزی‌های منظم امنیتی

انجام ممیزی‌های منظم امنیتی به شناسایی آسیب‌پذیری‌ها و اطمینان از به‌روزرسانی تدابیر امنیتی کمک می‌کند. ممیزی‌ها باید تمام جنبه‌های متاورس را شامل نرم‌افزار، سخت‌افزار و تعاملات کاربران و اجرای سیاست‌های تست نفوذ و ارزیابی‌های پوشش دهند.

۷-۱-۲ نظارت مداوم و پاسخ به حادثه

برپایی سیستم‌های نظارت مداوم می‌تواند به شناسایی فعالیت‌های غیرعادی و پاسخ به تهدیدات در زمان واقعی کمک کند. این موضوع شامل راه‌اندازی سیستم‌های مدیریت اطلاعات و رویدادهای امنیتی [۱] برای جمع‌آوری و تحلیل داده‌های امنیتی از منابع مختلف است. علاوه بر این، داشتن یک برنامه قوی پاسخ به حادثه که شامل روش‌های از پیش‌تعریف‌شده برای رسیدگی به نقض‌های امنیتی باشد، می‌تواند خسارات را به حداقل رسانده و بهبودی سریع را تضمین کند.

۷-۲ آموزش و آگاهی کاربران

۷-۲-۱ برنامه های آموزشی امنیتی

اجرای برنامه‌های آموزشی جامع امنیتی برای کاربران، برای افزایش آگاهی درباره تهدیدات احتمالی و شیوه‌های ایمن ضروری است. این برنامه‌ها باید موضوعاتی مانند تشخیص تلاش‌های فیشینگ، استفاده از رمزهای عبور قوی و فهم تنظیمات حریم خصوصی را پوشش دهند. به‌روزرسانی‌های منظم و دوره‌های بازآموزی می‌توانند کاربران را درباره آخرین روندهای امنیتی و تهدیدات مطلع نگه دارد.

[۱] Security information and event management(SIEM)

۷-۲-۲ مشارکت جامعه

مشارکت جامعه در تلاش‌های امنیتی می‌تواند فرهنگ مراقبت و مسئولیت‌پذیری را تقویت کند. تشویق کاربران به گزارش فعالیت‌های مشکوک و ارائه کانال‌های ارتباطی شفاف می‌تواند وضعیت امنیتی کلی متاورس را بهبود بخشد. ابتکارات جامعه‌محور، مانند انجمن‌های امنیتی و کمپین‌های آگاهی‌بخشی، نیز می‌توانند نقش مهمی در آموزش و توانمندسازی کاربران ایفا کنند.

۷-۳ همکاری و استانداردها

۷-۳-۱ همکاری صنعتی

همکاری بین ذینفعان صنعتی برای مقابله با چالش‌های پیچیده امنیتی متاورس حیاتی است. تشکیل اتحادیه‌ها و گروه‌های کاری می‌تواند تبادل بهترین شیوه‌ها، اطلاعات تهدیدات و نوآوری‌های امنیتی را تسهیل کند. این تلاش‌های مشترک می‌تواند به توسعه چارچوب‌ها و پروتکل‌های امنیتی استاندارد منجر شوند که به نفع کل زیست بوم باشند.

۷-۳-۲ توسعه استانداردها

توسعه و پذیرش استانداردهای امنیتی صنعتی می‌تواند تضمین‌کننده یک رویکرد هماهنگ برای حفاظت از متاورس باشد. این استانداردها باید جنبه‌های مختلف امنیتی از جمله حفاظت از داده‌ها، احراز هویت کاربران و پاسخ به حادثه را شامل شوند. نهادهای نظارتی و انجمن‌های صنعتی می‌توانند نقش مهمی در ایجاد و اجرای این استانداردها برای افزایش امنیت و اعتمادپذیری متاورس ایفا کنند.

۸ جمع‌بندی

متاورس پتانسیل عظیمی برای تحول در تعاملات دیجیتال دارد، امّا موفقیت آن به تدابیر امنیتی قوی بستگی دارد. با پرداختن به چالش‌های کلیدی امنیتی و اجرای راه‌حل‌های فناوری پیشرفته، می‌توان محیطی امن و قابل اعتماد برای کاربران ایجاد نمود. همکاری بین ذینفعان و استراتژی‌های امنیتی پیشگیرانه برای پیمایش در چشم‌انداز تهدیدات متغیر و تضمین موفقیت بلندمدت متاورس ضروری خواهد بود.

تکامل متاورس، تضمین امنیت آن برای موفقیت و پذیرش گسترده آن حیاتی است. با اجرای راه‌حل‌های قوی در فناوری، رسیدگی به مسائل قانونی و حکومتی، و ترویج یک فرهنگ امنیتی پیشگیرانه، می‌توان محیطی امن و قابل اعتماد برای همه کاربران ایجاد کرد. همکاری مداوم، نوآوری و هوشیاری، کلیدهای موفقیت در مواجهه با چالش‌های امنیتی و تحقق پتانسیل کامل متاورس خواهند بود.

۹ مراجع

۱- Rashid, Abeed. "Cybersecurity and the Metaverse: Patrolling the New Digital World."; (۲۰۲۲).

۲- Kshetri, N. "The rise of blockchains: disrupting economies and transforming societies". Edward Elgar Publishing; (۲۰۲۲).

۳- Huber, B. "The Role of Cybersecurity in the Future of the Metaverse". Tenable. Retrieved from Tenable;(۲۰۲۲).

٤- Wang, H., Ning, H., Lin, Y., Wang, W., Dhelim, S., Farha, F., ... & Daneshmand, M. "A survey on the metaverse: The state-of-the-art, technologies, applications, and challenges". IEEE Internet of Things Journal, ۱۰(۱٦), ۱٤٦۷۱-۱٤٦۸۸;(۲۰۲۳)

٥- Van Rijmenam, M. Step into the Metaverse:" How the immersive Internet will unlock a trillion-dollar social economy". John Wiley & Sons;(۲۰۲۲)

٦- https://www.esecurityplanet.com/trends/metaverse-security

۷- ۲٥ ,*فصلنامه تحقیقات حقوقی* .مرادی برلیان, مهدی. (۱٤۰۱). درآمدی بر پیامدها و چالش های حقوقی متاورس
doi: ۱۰,٥۲٥٤۷/jlr.۲۰۲۲,۲۲۸۲۸٦,۲۲۷۹ -. (ویژه نامه حقوق و فناوری), ۳٦۳-۳۹۲

نشانی: تهران، انتهای کارگر شمالی، پژوهشگاه ارتباطات و فناوری اطلاعات، معاونت پژوهش و توسعه ارتباطات علمی

تلفن: ۰۲۱-۸۸۶۳۰۳۵۵

نمابر: ۰۲۱-۸۸۶۳۰۳۵۶