ความท้าทายของการปกป้องตัวตนใน Metaverse

ปัจจุบัน Metaverse เข้ามามีบทบาทอย่างมากในภาคธุรกิจ ด้วยการช่วยเพิ่มประสิทธิภาพในการบริหารจัดการตลอดห่วงโซ่อุปทาน ตั้งแต่การออกแบบสินค้า ไปจนถึงการบริหารคลังสินค้า ทั้งนี้ Metaverse เป็นการผสานเทคโนโลยีแห่งโลกเสมือนที่สร้างสิ่งแวดล้อมของโลกจริง ๆ และเทคโนโลยีเข้าด้วยกัน เพื่อให้ผู้คนเข้ามามีปฏิสัมพันธ์และทำกิจกรรมร่วมกัน ผ่านตัวตนที่เป็นอวตาร (Avatar) ในรูปแบบกราฟิก 3 มิติ แทนเราในการทำกิจกรรมต่าง ๆ ทำให้รู้สึกเหมือนชีวิตจริงมากกว่าโซเชียลมีเดียที่ใช้อยู่ นอกจากนี้ Gartner ยังคาดการณ์ว่าภายในปี 2027 องค์กรขนาดใหญ่กว่า 40% ทั่วโลกจะใช้ Web3, Spatial Computing และ Digital Twins เพื่อเพิ่มรายได้ ผ่านโครงการ Metaverse ดังนั้น Metaverse จึงก่อให้เกิดโอกาสใหม่ ๆ มากมาย แต่ก็ยังเป็นความท้าทายในเรื่องการรับรองความปลอดภัยทางไซเบอร์ของผู้ใช้ โดยเป้าหมายสำคัญคือ การปกป้องตัวตนดิจิทัลใน Metaverse

ทั้งนี้แนวคิดของตัวตนดิจิทัลมีการใช้งานอยู่แล้ว ซึ่งเป็นข้อมูลทั้งหมดที่มีอยู่บนอินเทอร์เน็ตเกี่ยวกับผู้ใช้แต่ละคน ซึ่งสร้างขึ้นจากการเคลื่อนไหวบนโลกอินเทอร์เน็ต เช่น การใช้โซเชียลเน็ตเวิร์ก การมีส่วนร่วมในฟอรัมต่าง ๆ การซื้อสินค้าในร้านค้าออนไลน์ เป็นต้น ทั้งหมดเหล่านี้จะเป็นสิ่งที่ Metaverse ใช้ในการกำหนดตัวตนและสร้างตัวแทนของผู้ใช้แต่ละคนหรือที่เรียกว่า อวาตาร์ เพื่อการมีส่วนร่วมในโลกเสมือนจริง ดังนั้นจึงมีความเป็นส่วนตัวที่จะต้องปกป้อง เช่น สิทธิ์ในรูปภาพ และความเป็นส่วนตัวในโลกจริง เป็นต้น

การปกป้องตัวตนใน Metaverse

ปัจจุบันการควบคุมรอยเท้าบนโลกดิจิทัล (Digital Footprint) เป็นงานที่ซับซ้อนมาก และเมื่อมี Metaverse เข้ามา ทำให้ความยากเพิ่มมากขึ้น เนื่องจากอุปกรณ์หลายชิ้นถูกใช้เพื่อรวบรวมข้อมูลจำนวนมากในพื้นที่เสมือนจริง สามารถติดตามการเคลื่อนไหวของร่างกาย คลื่นสมอง และการตอบสนองทางสรีรวิทยา ผู้ใช้สามารถโต้ตอบและสร้างข้อมูลเพิ่มเติมสำหรับใช้ในงานต่าง ๆ เช่น การปรับปรุงประสบการณ์ของผู้ใช้ ดังนั้น ในการปกป้องข้อมูลประจำตัวดิจิทัลและหลีกเลี่ยงความเสี่ยงต่าง ๆ คือการใช้ Sovereign Digital Identity หรือที่เรียกว่า ข้อมูลประจำตัวดิจิทัลที่มีอำนาจอธิปไตย โดยแนวคิดนี้อิงตามเทคโนโลยี Blockchain และช่วยให้ผู้ใช้สามารถโต้ตอบในสภาพแวดล้อมเหล่านี้ได้ ในขณะที่รับรู้ว่าข้อมูลใดถูกแบ่งปันและแบ่งปันกับใครบ้าง ด้วยระบบนี้ ผู้ใช้สามารถระบุตัวตนได้อย่างปลอดภัย โดยไม่ต้องเปิดเผยข้อมูลมากเกินไป อีกทั้งยังช่วยในการรับประกันความเป็นส่วนตัวและความปลอดภัย นอกจากนี้การออกแบบโปรแกรมการยอมรับที่ครอบคลุม จะช่วยให้ผู้ใช้สามารถจะยอมรับหรือไม่ประมวลผลข้อมูลของตนทั้งหมด ทั้งนี้การป้องกันตัวตนจะครอบคลุมถึงรหัสผ่าน การเข้าสู่ระบบไบโอเมตริกซ์ การยืนยันตัวตนแบบหลายปัจจัย (MFA) และการเข้ารหัสจากต้นทางถึงปลายทาง เป็นต้น

6 ปัจจัยในการพิจารณาเพื่อดำเนินการเกี่ยวกับ Metaverse

1. การปรับปรุงกลไกการยินยอม ผู้ใช้ต้องได้รับการศึกษาเกี่ยวกับความเป็นส่วนตัว และควรได้รับการปรับปรุงความยินยอมเป็นประจำ โดยไม่กำหนดให้ความยินยอมเป็นการอนุญาตแบบถาวร

2. แจ้งผู้ใช้เมื่อพวกเขาโต้ตอบกับ AI เพื่อความโปร่งใสอย่างสมบูรณ์ บอท AI จะต้องติดป้ายกำกับเพื่อให้ผู้ใช้ทราบว่ากำลังแบ่งปันข้อมูลกับใคร

3. การควบคุมตนเอง ปัจจุบันกฎหมายความเป็นส่วนตัวไม่สอดคล้องกันทั่วโลก ว่ากำลังแบ่งปันข้อมูลกับใคร ดังนั้น บริษัทต่างๆ จะต้องควบคุมตนเองเพื่อรักษาความไว้วางใจของผู้บริโภค

4. ความโปร่งใสในการใช้ข้อมูล โดยเฉพาะการใช้ข้อมูลในอินเทอร์เน็ตเพื่อสร้างรายได้ ดังนั้นบริษัทจะต้องแสดงความโปร่งใสเกี่ยวกับวิธีการใช้ข้อมูล รวมถึงการชดเชยให้กับผู้ใช้งานในกรณีที่มีการรวบรวมข้อมูลของพวกเขาไว้เพื่อใช้ประโยชน์

5. การป้องกันข้อมูลส่วนตัวควรใช้งานง่าย บริษัทควรดำเนินการต่ออายุความยินยอมในทุกจุดที่ผู้ใช้งานต้องป้อนข้อมูลเข้าไปใหม่ แม้จะเป็นการตรวจสอบสิทธิ์เพิ่มเติมก็ตาม

6. โลก VR ต้องคำนึงถึงความปลอดภัยของข้อมูล การใช้บริการ Metaverse จะมีการเก็บข้อมูลจำนวนมหาศาล ดังนั้นแพลตฟอร์มที่ให้บริการจะต้องมีมาตรการการดูแลและควบคุมข้อมูลไม่ให้มีการรั่วไหลและใช้หลักการเข้ารหัสที่มีความปลอดภัย

เทคโนโลยีการรักษาความปลอดภัยของข้อมูล

- **Firewalls** เป็นซอฟต์แวร์หรือฮาร์ดแวร์ บนระบบเครือข่าย ทำหน้าที่ตรวจสอบข้อมูลที่ผ่านเข้า-ออกระบบเครือข่าย คัดกรองข้อมูลที่เข้ามาว่าเป็นข้อมูลอะไร มาจากที่ไหนและจะส่งไปที่ใด เพื่อเป็นการป้องกันว่าข้อมูลที่จะส่งผ่านเข้ามานั้นมีความปลอดภัยหรือไม่ ด้วยการกำหนดกฎ (Rule) หรือนโยบาย (Policy) ของผู้ดูแลระบบ หากข้อมูลไม่ตรงตามกฎที่กำหนดไว้ ระบบ Firewall ก็จะไม่ยอมให้ผ่านเข้าไปได้

- **Authentication and Authorization**

Authentication เป็นระบบยืนยันตัวตนที่เมื่อเราจะเข้าใช้งานในเว็บไซต์ แอปพลิเคชั่นหรืออะไรก็ตามบนโลกออนไลน์จะต้องมีการ Login เข้าระบบก่อน เพื่อยืนยันตัวตนและตรวจสอบสิทธิ์ว่าผู้ใช้งานระบบนั้นมีสิทธิ์ใช้ได้และเป็นเจ้าของข้อมูลนั้นจริงๆ

Authorization เป็นระบบการรักษาความปลอดภัยที่ระบุและกำหนดระดับการเข้าถึงหรือสิทธิ์ของผู้ใช้ผ่านตัวตนที่ได้ Login เมื่อระบบทราบว่าเราเป็นใครระบบก็จะทำการ Authorization เพื่อตรวจสอบว่าเรามีสิทธิ์จะเห็นหรือจะทำอะไรได้บ้าง ซึ่งถือเป็นอีกขั้นตอนของการทำ Authentication นั่นเอง ในระดับองค์กร การใช้ Authorization เพื่อระบุว่าพนักงานคนไหนสามารถเข้าถึงหรือใช้ข้อมูลได้ในระดับใด เพื่อให้มั่นใจในเรื่องการเข้าถึงสิทธิ์ข้อมูลที่บริษัทต้องการรักษาความลับ

- **Encryption** เป็นการเข้ารหัสข้อมูล โดยการเปลี่ยนแปลงข้อมูลเพื่อไม่ให้ผู้อื่นสามารถแปลความหรือไม่ต้องการให้เข้าใจข้อมูลนั้น ๆ เช่น เปลี่ยนข้อความทั่วไปให้เป็นรหัส ()J*@KF)POUBNJIFG

- **Data Masking** เป็นกระบวนการปกป้องข้อมูลที่ไม่ใช่การเข้ารหัส แต่เป็นการทำให้ข้อมูลที่แสดงเป็นข้อมูลหลอกหรือนาแฝง ทั้งนี้เพื่อปกปิดข้อมูลจริง เช่น ชื่อ อีเมล์ วันเดือนปีเกิด หมายเลขบัตรประชาชน เบอร์โทรศัพท์ เป็นต้น โดยระบบจะทำการปกปิดข้อมูลเมื่อจำเป็นต้องมีการส่งออกข้อมูลไปยังหน่วยงานภายนอกไม่ส่งออกเป็นไฟล์ หรือผ่าน API

- **Hardware-based security** เป็นการรักษาความปลอดภัยทางไซเบอร์ให้กับฮาร์ดแวร์ เพื่อช่วยปกป้องการโจมตีที่อาจเกิดขึ้น การรักษาความปลอดภัยที่สนับสนุนด้วยฮาร์ดแวร์ใช้แนวทางที่ครอบคลุมหลายมิติ ไม่เพียงแต่ช่วยเสริมการรักษาความปลอดภัยที่สนับสนุนด้วยซอฟต์แวร์ แต่ยังเพิ่มประสิทธิภาพในการใช้และจัดการการป้องกันโครงสร้างพื้นฐานในการประมวลผลด้วย

- **Data backup and resilience** เป็นการสำรองข้อมูลเพื่อป้องกันการประสบปัญหาข้อมูลสูญหายหรือถูกโจมตี ต้องมีการวางแผนการสำรองข้อมูลและควรมีความยืดหยุ่นในการจัดการข้อมูลเหล่านั้นด้วย

- **Data Erasure** เป็นกระบวนการลบข้อมูลที่ได้รับการยอมรับโดยการใช้ซอฟต์แวร์ในการเขียนทับข้อมูลที่มีอยู่แล้ว บนฮาร์ดดิสก์ไดรฟ์หรืออุปกรณ์ IT อื่นๆ เพื่อทำการลบข้อมูลทั้งหมด ซึ่งเป็นการล้างข้อมูลเพื่อให้ยากต่อการกู้ข้อมูลกลับมาใช้ใหม่ได้ จนไม่สามารถกู้กลับคืนมาได้เลย

Reference

https://www.xrtoday.com/virtual-reality/metaverse-data-protection-and-privacy/

https://martechvibe.com/martech/data-privacy-in-metaverse-is-an-evolving-concern/

https://venturebeat.com/virtual/why-privacy-and-security-are-the-biggest-hurdles-facing-metaverse-adoption/

https://www.telefonica.com/en/communication-room/blog/how-to-protect-digital-identity-in-the-metaverse/

https://www.techtarget.com/searchsecurity/feature/Top-7-types-of-data-security-technology

https://monsterconnect.co.th/authentication-vs-authorization/