TAGESSPIEGEL
BACKGROUND

Cybersecurity

Reale Risiken in virtuellen Realitäten

Lang ist die Liste potenzieller Verbrechen im Metaverse. Fachleute sowie Interpol und Europol warnen vor allem vor Finanzdelikten wie Betrug, Geldwäsche oder dem Diebstahl von Kryptowährungen, Daten und Identitäten. Mikko Hyppönen, langjähriger Forschungschef von Withsecure, hat eine eigene Sicht.

von **Ulrich Hottelet**

veröffentlicht am 11.07.2023

„Viele Anwendungsfälle im **Metaverse**, an die Leute denken, sind Spiele in einem Umfeld wie Minecraft. Ich denke aber nicht, dass wir in virtuellen Welten leben werden. Spielen in virtuellen Welten wird überschätzt, Arbeiten dort wird unterschätzt“, sagt der renommierte Sicherheitsexperte **Mikko Hyppönen**, Chief Research Officer bei der finnischen Cybersicherheitsfirma **Withsecure**. Erinnert man sich an den Hype um **Second Life**, das in der Versenkung verschwunden ist, so könnte Hyppönen durchaus Recht behalten. Dementsprechend sieht er die Risiken vor allem in der Arbeitswelt.

„Wenn Sie mit Excel arbeiten oder programmieren und einen VR-Helm aufsetzen, gibt es keine begrenzte Zahl an Bildschirmen wie am Schreibtisch. Außerdem haben die Bildschirme eine bessere Qualität“, sagt er. Die Mitarbeitenden würden daher eine solche **Arbeitsumgebung** bevorzugen. Der Grund dafür, dass der VR-Einsatz in der Berufswelt noch nicht gängig ist, sei die Bildauflösung, die sich erst in letzter Zeit deutlich verbessert habe.

Da Hyppönen das Metaverse für keine digitale Revolution in unserem Leben hält, findet er auch dessen Risiken **nicht grundsätzlich neu**. Welche die relevantesten und realistischsten sind, sei schwer zu beurteilen. Er erwartet, dass sich zunächst bereits **bekannte Betrugsmaschen** mit der Liebe und Auktionen sowie fingierte Appelle von Angehörigen verbreiten, die wegen eines Notfalls um Geld bitten. Er sagt: „Das kann schnell auf das Metaverse ausgedehnt werden. Consumer-to-Consumer-Betrügereien werden wir als Erstes sehen. In der Geschichte des Internets nimmt die Online-Kriminalität immer erst die Verbraucher ins Visier und später dann die Unternehmen.“

Polizeipräsenz in der VR-Umgebung

Eine zentrale Bedrohung sieht er interessanterweise im Metaverse selbst, nämlich im dann technisch möglichen **Ausspionieren der Nutzer:innen** durch die Betreiberfirmen. Er vermutet, dass Facebooks Mutterkonzern Meta Milliarden Dollar in das Metaverse investiert, um sein lukratives **Werbegeschäft** noch weitaus besser personalisieren zu können. „Im Metaverse können die Betreiber wirklich wissen, wen du liebst und hasst“, so Hyppönen. Denn die **Vergrößerung der Netzhaut in Reaktion** auf das Gesehene sei durch die Kamera im VR-Helm erkennbar. „Dabei kann man nicht täuschen. Das tötet die Privatsphäre ultimativ!“ Da der Konzern die Zustimmung dazu im Kleingedruckten der AGBs verstecken könnte, wie Hyppönen vermutet, wäre das nicht einmal illegal.

Ein **Bericht von Europol zum Metaverse** aus dem vergangenen Jahr (*PDF, 29 Seiten (https://www.europol.europa.eu/cms/sites/default/files/documents/Policing%20in%20the%20metaverse%20-%20what%20law%20enforcement%20needs%20to%20know.pdf)*) geht von vielen möglichen Kriminalitätsformen aus, beispielsweise **Geldwäsche**, sexuelle **Belästigung** und **Ransomware-Attacken**

auf digitale Vermögenswerte. Auch vor Diebstahl von biometrischen Informationen etwa zur Begehung von Betrugsdelikten oder zur Herstellung von Deepfakes warnt die Polizeibehörde. Laut Medienberichten sollen Cyberkriminelle ihre Opfer mit Deepfakes von Kryptowährungsfachleuten bereits zu virtuellen Treffen gelockt haben. Sicherheitsexpert:innen befürchten, dass zur Vorbereitung von Straftaten auch in der virtuellen Welt Mittel wie **Phishing**, Social Engineering und Man-in-the-Middle-Angriffe eingesetzt werden.

Mit Verweis auf die Gefahren brachten Bayern und Sachsen-Anhalt Ende Mai einen Antrag auf der Justizministerkonferenz ein, in dem die beiden Länder Bundesjustizminister Marco Buschmann (FDP) aufforderten zu prüfen, an welchen Stellen **das Straf- und Strafprozessrecht angepasst** werden müsse. Hyppönen zeigt sich bezüglich gesetzgeberischer Initiativen reserviert: „Die **Gesetze gelten auch für Virtual Reality**. In den letzten 30 Jahren wurden Gesetze bewusst so allgemein formuliert. Ich hoffe, dass neue Regeln nicht notwendig sein werden."

Sozusagen proaktiv geht **Interpol** vor. Zum einen untersucht die Polizeiorganisation Methoden, wie Verbrechen im Metaverse überwacht werden können. Zum anderen hat sie sogar eine **eigene VR-Umgebung** entwickelt, in der sie Strafverfolgungsbehörden eine Vorschau auf mögliche Arten von Verbrechen bietet und wo Mitarbeitende Schulungen erhalten und virtuelle Meetings abhalten können (Tagesspiegel Background *berichtete (https://background.tagesspiegel.de/cybersecurity/metaverse-interpol-eroeffnet-digitale-repraesentanz)*). Interpol erklärt auf seiner Website dazu: „Das Metaverse hat viele Vorteile für die Strafverfolgung, insbesondere in der Telearbeit, der Vernetzung, dem Sammeln und Aufbewahren von Beweismitteln und im Training."

Digitale Zwillinge im Visier

Viel beschworen wird in Fachkreisen auch die Gefahr der *Desinformation (https://background.tagesspiegel.de/cybersecurity/desinformation-im-metaverse-kommt-die-digitale-dystopie)*. Videos sind **manipulierbar**, virtuelle Influencer können falsche Informationen verbreiten und **Deepfakes** können zum Beispiel Prominenten falsche Botschaften in den Mund legen. Hyppönen findet diese Bedrohung aber nicht so groß. „In der Virtual Reality sieht man nicht gleich aus wie im echten Leben. Avatare ähneln uns nur. In VR gehen wir schon davon aus, dass alles ein Avatar ist, gerendert ist und **nichts real** ist." Auch mit dem Begriff Deepfake im Zusammenhang mit dem Metaverse ist er zurückhaltend. „Man kann einen Avatar klonen, aber das ist noch kein Deepfake. Vielleicht wird es aber in Zukunft so sein, dass Avatare sehr realistisch aussehen und man dann von Deepfakes sprechen kann."

Ins kriminelle Visier können auch **Digitale Zwillinge** geraten, und das in zweifacher Hinsicht. Zum einen besteht die Möglichkeit, in den virtuellen Räumen die Baupläne von Digitalen Zwillingen einzusehen. Die Wirtschaftsprüfungs- und Beratungsgesellschaft PwC *warnt (https://www.pwc.de/de/im-fokus/cyber-security/neue-risiken-an-der-schnittstelle-von-metaverse-und-digitalen-zwillingen.html)* auch vor „**Data Poisoning**, bei dem die Daten der zugrundeliegenden KI- und Machine-Learning-Systeme bewusst verfälscht werden. Damit werden die Erkenntnisse aus Simulationen nicht nur unbrauchbar, sondern können im schlimmsten Falle auch zu fatalen Geschäftsentscheidungen auf Basis der verzerrten Ergebnisse führen.

Zum anderen dehnt PwC den Begriff des Digitalen Zwillings, der sich üblicherweise auf Objekte, Prozesse und Dienstleistungen bezieht, auf Menschen beziehungsweise deren Avatare aus. „Kriminelle können über die Manipulation von Digitalen Zwillingen **Identitätsdiebstahl** betreiben, **Betriebsgeheimnisse** ausspähen, Daten verschlüsseln, Unternehmen erpressen und unter falscher Identität illegalen Geschäften nachgehen", schreibt PwC und skizziert ein Szenario, in dem Kriminelle via Social Engineering mit gefakten Digitalen Zwillingen ihre Opfer täuschen, zum Beispiel indem sie Führungskräfte oder Konferenzräume im virtuellen Raum imitieren und unwissende Mitarbeiter:innen zur Preisgabe sensibler Informationen bewegen.

Auch in einer *Untersuchung (https://documents.trendmicro.com/assets/white_papers/wp-metaverse-or-metaworse-cybersecurity-threats-against-the-internet-of-experiences.pdf)* (PDF, 24 Seiten) des japanischen Cybersicherheitsunternehmens **Trend Micro** wird vor Gefahren für Digitale Zwillinge gewarnt: Wer im

Metaverse direkt oder nur schlecht geschützt einen Digitalen Zwilling erreichbar macht, gibt solche **Baupläne** möglicherweise auch an Kriminelle weiter, warnt der Bericht. Wenn es Angreifenden beispielsweise gelingt, sich Zugang zum Digitalen Zwilling eines Kraftwerks zu verschaffen, könnten sie die **Kommando- und Kontrollnetze** unrechtmäßig manipulieren. Auch könnten Kriminelle sich durch das Metaverse digitale **Blaupausen des Geländes** konstruieren, um einen physischen Angriff zu planen (Tagesspiegel Background *berichtete (https://background.tagesspiegel.de/cybersecurity/metaverse-zwischen-hype-und-cyberrisiken)*).

Auf die realen Risiken konzentrieren

Was können wir nun tun, um die sich abzeichnende Kriminalität im Metaverse zumindest einzudämmen? „Das ist schwer zu sagen. Die **Strafverfolgungsbehörden und Regierungen** sollten sich mit der neuen Technologie beschäftigen und sie verstehen, um die Gefahren herauszufinden", sagt Hyppönen. **Bildung und Awareness-Programme** hält er für die „wahrscheinlich besten Mittel", fügt aber hinzu: „Wir sollten die Menschen nicht zu sehr in Schrecken versetzen und uns stattdessen auf die realen Risiken konzentrieren."

Während die Gefahren im Metaverse eher mittel- bis langfristig sind, hält der Forschungschef kurzfristig die Risiken rund um **Augmented Reality** für relevanter. Denn Kriminelle können die durch AR verfügbaren Infos nutzen, um Dinge **falsch zu beschreiben**. „Ein Konkurrent kann in Google Maps Ihren Laden als geschlossen markieren oder mit einem schlechten Ranking versehen. Das ist kein Riesenproblem, aber es passiert bereits."