BIZCOMMUNITY

The metaverse reality check that businesses need

By Pankaj Bhula

9 Sep 2022

The metaverse will transform the way that companies operate. Gartner predicts that by 2026, a quarter of us will spend at least one hour a day in the metaverse for work, shopping, education, social media and/or entertainment. Some brands are already there today, such as Nike and Coca-Cola, who are using them to drive brand awareness and the purchase of physical products.

Source: © ismagilov – 123RF.com

With so much buzz around the metaverse, it's easy to see why more and more companies will start to do business there. But are they thinking about the risks? We will certainly need a different approach to security in a virtual world compared to the physical, but what will that entail? Let's take a look at what the risks are and how to start getting prepared (because you do need to start now).

The biggest hurdle to the metaverse being a secure environment is in its foundations. The metaverse is built on blockchain technology and we have already seen serious security gaps in NFT marketplaces and blockchain platforms such as OpenSea, Rarible and Everscale. Due to the sheer amount of malicious activity that we already see exploiting services based on the blockchain, we believe it won't be long before we start to see initial attacks in the metaverse too. It will likely be based on authorisation, and user accounts will get hijacked, so we expect that identity and authentication will sit at the heart of everything we want to do.

It is tricky though, as people might want to have multiple identities within the metaverse, perhaps one for transacting work conversations and another for personal shopping and entertainment. This adds another layer of complexity because there's then no single identity that says it's definitely you. The answer could be in chained identity so, will blockchain then help us understand where we're transacting and who with? This is a major challenge. And since blockchain technologies are decentralised and unregulated, this makes things like policing the theft of virtual assets or preventing money laundering, very difficult indeed.

Redefining reality

Another key security challenge is in the safe spaces needed to conduct business. Imagine you're on a Zoom or Teams call. It's a private meeting space, right? But what will that be like in the metaverse? How do we know that a chair someone is sitting on isn't actually an avatar and we have an impostor in our midst? You may think that can't possibly happen, but it's a virtual world. Of course, it can. We need to be able to discern between what's real and what's fake, and having a safe space to meet and transact will be crucial.

When the Internet first came out, threat actors exploited the average human's unfamiliarity with the tech by creating malicious sites that impersonated banks to obtain financial details. Phishing scams like this still occur, albeit we now see more sophisticated forms of social engineering. The metaverse is like a whole new Internet, and you can guarantee that people's unfamiliarity with it, both businesses and consumers, will be exploited.

Interestingly, every transaction that happens on the blockchain is fully traceable, so this will become far more important, especially when it comes to having an audit trail of what has been discussed and any decisions made in a business context. But that leaves a question over how that information is taken from the virtual world to the physical. Are contracts going to be legally binding in the metaverse? Or will they need to be brought into the physical world to be signed and then pushed back in? How will that be done securely?

Researchers have discovered security gaps within blockchain and crypto projects which are part of the metaverse. The vulnerabilities that been exploited by cybercrime are focused on vulnerabilities with smart contracts that allows hackers to exploit and drain crypto platforms and around application vulnerabilities inside blockchain platforms that allows hackers to attack through the platforms and hijack users' wallets balance. There is a danger that we rush headlong into the metaverse without considering these types of implications.

A lot of the concerns around security in the metaverse are exacerbated by the huge skills shortage in the cybersecurity sector. According to the 2021 (ISC)² Cybersecurity Workforce Study, we are lacking almost 3 million cybersecurity professionals and the current global cyber workforce needs to grow by 65% to effectively defend organizations' critical assets. That percentage is likely to be a lot higher if we also consider the new virtual world.

Is it worth it?

Other cybersecurity risks within the metaverse abounds such as cyberattacks via the use of vulnerable AR/VR devices, as an entryway for evolving malwares and data breaches. These devices inherently collect large amounts of user data and information such as biometrics, making it attractive to hackers. Concerns around data privacy are also a growing voice amongst metaverse sceptics, with additional data being collected through avenues like Second Life, potentially violating user privacy.

You might be reading this thinking well, why bother if there are so many risks involved? But it is absolutely worth putting the time in now, to get ready for moving across to the metaverse. Unfortunately, any company (no matter the size) that doesn't, may find itself in a place where it's playing catch up and potentially losing out on business or engaging in processes that put the business at risk. You can transition slowly, just like many have done with cloud migration.

Organisations will need to be much more reliant on their partners around the world to help mitigate risk, as this is very much a global phenomenon. But there will always be some risk and for those that take them and get it right, there will be huge rewards. At the end of the day though, businesses won’t be able to do it themselves, it will take a great deal of partnering with organizations that work within that space. The metaverse will hit everyone, and there’s no denying that mistakes will be made, similar to those that were made in the early days of the Internet.

Top metaverse security considerations right now:

It's coming. You can't put your head in the sand and pretend that it isn't. Business leaders and security professionals need to talk about it and understand what it might mean for them. Understand the landscape by looking at what competitors are doing in that space.
Have a look at how you are currently running services now in the physical world and understand if these services map in any way to the metaverse. You may find that some of them don't and aren't even secure in this world, such as mobile devices, tablets, cloud and multi-cloud.

Understand how to get your identification and authentication done correctly. The answer to that isn't just having a password or two-factor authentication. Companies need to really start upping their game around these two issues. People tend to do things without thinking about security, whereas they should be thinking of security first.

ABOUT THE AUTHOR

Pankaj Bhula is Check Point's EMEA regional director: Africa.