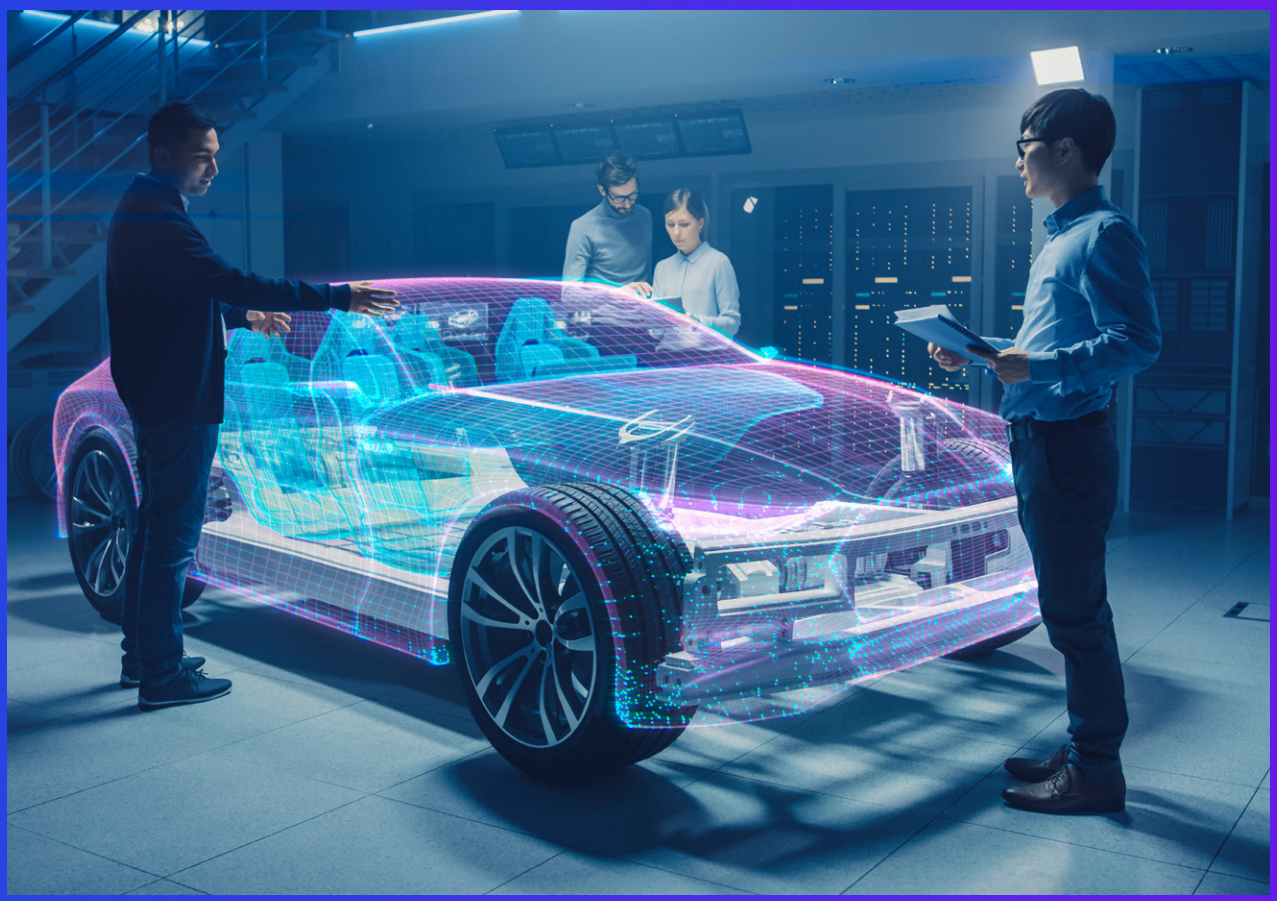
KPMG

Considerações Cibernéticas para o Metaverso



Abril de 2023

kpmg.com

Quatro considerações cibernéticas para líderes de segurança

1. Personificação digital
2. Interoperabilidade
3. Risco de invasão de conta — ataque de repetição de credenciais
4. Proteção de dados/uso indevido

A próxima evolução da Internet já começou e atende pelo nome de "metaverso". Conforme o escopo da Internet se expande, as experiências do usuário se tornam mais imersivas graças à realidade virtual, onde a realidade aumentada permite aprimorar as emulações dos espaços físicos por meio de detalhes e complementos virtuais. É como se, no metaverso, recriássemos o mundo tal como o conhecemos, mas sem as limitações impostas, por exemplo, pelo distanciamento geográfico; neste exato momento, milhões de pessoas ao redor do mundo estão trabalhando para viabilizar experiências metaversas cada vez mais realistas, imersivas e surpreendentes.

No mundo corporativo, o metaverso abre caminhos para o crescimento das empresas, o aprimoramento da interação com os clientes e uma transformação profunda nas estruturas de custos. As oportunidades de crescimento continuarão a surgir à medida que as interações digitais se tornarem mais imersivas e contextuais

Entretanto, quando olhamos através das lentes da segurança cibernética, percebemos que essas novidades instigantes não estão isentas de riscos. Com a expansão dos limites da Internet, os cibercriminosos encontram cada vez mais espaços vulneráveis para explorar. Além disso, o crescente realismo dessas experiências acarreta preocupações adicionais de segurança e proteção, uma vez que os usuários veem, ouvem e sentem tudo de uma maneira mais impactante do que na interação digital tradicional.

Nesse momento de disrupções tão impactantes, os líderes de segurança desempenham papel de destaque nas ambições metaversas de qualquer organização. São eles que, ao se engajarem ativamente em trazer iniciativas de metaverso para os mercados, têm a incumbência de proteger tanto os clientes quanto os investimentos de suas respectivas empresas. Assim, são fundamentais para estabelecer a confiança necessária ao sucesso dessas iniciativas.

Uma coisa é certa: segurança digital bem-estruturada é essencial à construção da confiança dos *stakeholders*; e essa confiança é o alicerce do crescimento e da jornada de inovação realmente sustentável, tanto em termos de desempenho como de eficiência.

Então, quais são algumas considerações de risco que os líderes de segurança e os inovadores do metaverso precisam considerar?

1 Personificação Digital

- A identidade tem sido um desafio dentro da segurança digital, sendo um elemento central para a construção da confiança. As decisões de conceder acesso a recursos ou de autorizar ações – como transferir fundos ou assinar um contrato de locação – são tomadas com base na certeza de que "você é quem você diz ser". Essa certeza depende da solidez dos instrumentos e meios de verificação e asseguração de identidade."
- Os ataques de *phishing* e engenharia social continuam a ameaçar fortemente o ecossistema digital atual. O risco de cibercriminosos se passarem por seu gerente de conta, seu consultor virtual pessoal ou seu chefe/colega, e de darem instruções para executar tarefas maliciosas no ambiente virtual, existe e gera preocupações em todo tipo de organização.
- Técnicas de *deepfakes* também estão em ascensão. Em um espaço virtual, com o uso de *software* modulador de voz, torna-se cada vez mais fácil emular uma pessoa, inseri-la em montagens convincentes e vitimizá-la e/ou usá-la para vitimar terceiros.
- Adicionalmente, as experiências virtuais oferecem oportunidades para cibercriminosos cometerem fraudes de maneiras cada vez mais criativas. Por exemplo, imagine que você assista a um *show* virtual e pague um valor extra pelo direito de fazer uma visita virtual aos bastidores, para conhecer seu ídolo, fazer perguntas e trocar impressões. Um organizador mal-intencionado pode fazer com que pessoas comuns finjam ser o cantor, criando vários eventos de bastidores falsos. Então, em vez de vender uma dúzia ou mais de passes nos bastidores, esse agente poderia vender milhares de falsas interações e colher grandes lucros. Além de lesar os compradores, esse tipo de golpe poderia lançar uma sombra sobre as empresas que organizam eventos legítimos nos bastidores e prejudicar, dessa forma, todo um nicho do mercado de entretenimento. Um exemplo extremo seria um show inteiro tocado por um imitador, com fraudadores cobrando dos fãs que, sem saber, estariam prestigiando – e pagando caro – por um *deepfake*.

Considerações

Para os provedores de plataformas de metaverso, lembramos que:

• É essencial trabalhar para tornar os mecanismos de verificação de identidade absolutamente sólidos e refratários a ataques.

• Os consumidores devem ser capazes de interagir com seus criadores preferidos e permitir a troca de ativos digitais com o respaldo de uma verificação de identidade confiável, da mesma forma que as instituições financeiras blindam ao máximos os riscos relacionados à identidade de seus clientes.

• Vale a pena aproveitar inovações e integrações com protocolos de autenticação sem senha, a exemplo de credenciais FIDO (veja box) ou credenciais verificáveis (VCs), que permitem autenticação mais forte e reduzem o risco de ataques de *phishing* e engenharia social.

FIDO (*Fast ID Online*) é um conjunto de especificações de segurança independentes de tecnologia para autenticação forte. É desenvolvido pela FIDO Alliance, uma organização sem fins lucrativos que busca padronizar a autenticação nas camadas do cliente e do protocolo.

Para os consumidores, vale ressaltar:

• Considere plataformas e empresas conectadas no ecossistema, que ofereçam autenticação multifator e protocolos de verificação de identidade, especialmente para transações ou interações de maior risco, como movimentação de dinheiro.

• Informe-se, com antecedência, sobre as formas de descobrir se uma identidade pode ser fraudulenta e/ou não validada. Do mesmo modo que golpistas se passam por amigos e parentes de usuários de redes sociais para, por exemplo, pedirem dinheiro, conceitos semelhantes serão adotados no metaverso.

• Caso a plataforma de metaverso que você estiver usando não tenha o nível adequado de salvaguardas, redobre a atenção: o risco de ser alvo de fraudadores e pessoas mal-intencionadas pode ser maior

Dependência

Embora existam centenas de plataformas de interação metaversa, a interoperabilidade e a cocriação serão fatores críticos para que os consumidores levem seus avatares e identidades digitais para diferentes ambientes digitais. As autoridades em segurança digital e os diversos *players* que se propuserem a atuar no metaverso precisam trabalhar juntos para estabelecer protocolos de interoperabilidade e governá-los. Trata-se um grupo de atores bastante vasto, que inclui provedores de nuvem, pesquisadores de segurança, gigantes da tecnologia, provedores de serviços de Internet (ISPs) e outros – todos com um papel fundamental na habilitação de um ambiente seguro e interoperável entre metaversos.

2 Interoperabilidade

Entre os especialistas, predomina a visão de que o metaverso só poderá atingir massa crítica quando as questões de interoperabilidade e portabilidade estiverem resolvidas. Alguns apontam a tendência centralizadora das grandes empresas de tecnologia como entraves a essa diversificação – e até consideram o comportamento dessas organizações como contrário aos princípios fundamentais da *Web3* (veja *box*).

No entanto, independentemente de quem esteja conectando vários metaversos (centralizados ou descentralizados), a possibilidade de trazer seu avatar, sua identidade digital e seus ativos, como *token* não fungíveis (*NFTs*) e criptomoedas, cria riscos importantes de segurança e fraude para o ecossistema mais amplo.

Como já observado nos grandes ataques realizados nas *crypto "bridges",* construir conexões seguras e resilientes é essencial para manter a confiança. É igualmente necessária a autorregulação e a criação de normas de base de segurança para permitir a interoperabilidade em um ambiente seguro.

Ter um conjunto definido de princípios para evitar certos tipos de ataques em vários metaversos será um passo crítico – e, para que ele seja possível, é imperativo que as empresas trabalhem juntas. Pagar uma certa quantia de dinheiro por um ativo exclusivo em um metaverso que está vinculado à sua identidade e descobrir que ele foi roubado em um ambiente diferente, com menor segurança e mecanismos fracos de prevenção a fraudes, criaria rupturas irreversíveis em como a interoperabilidade seria mantida e corroeria a confiança no ecossistema mais amplo.

Web3 é a terceira geração da Internet, que se baseia na ideia de que a internet deve ser executada em uma rede de computadores descentralizada.

> O valor de ser uma empresa confiável para clientes, parceiros de negócios e reguladores é especialmente importante neste mundo de realidade mista e tecnologias disruptivas.

3 Risco de invasão de conta - ataque por meio da repetição de credenciais

O desenvolvimento e a integração de *bots* no metaverso, bem como o aumento da superfície de ataque, podem levar a novas maneiras de capturar ou roubar credenciais e segredos do usuário. À medida que a economia do metaverso floresce, as pessoas tendem a usar o espaço virtual para comprar ou vender seus produtos – e, assim, haverá muita movimentação de dinheiro.

Nesse ambiente, a aquisição de contas e a transferência de ativos para contas desonestas podem proliferar. Perder o acesso à sua identidade digital em um metaverso interconectado terá um impacto semelhante ao de, hoje em dia, perder o acesso à sua conta do Google. Os agentes mal-intencionados obterão acesso imediato ao seu histórico de pesquisa, histórico de localização e e-mails, podendo causar danos graves ao acessar contas de mídia social ou detalhes bancários. No futuro, porém, eles podem ter acesso a ativos exclusivos e carteiras de criptografia para transferir dinheiro e ativos valiosos, enquanto você perde o controle sobre sua identidade digital. Restaurar uma conta roubada exige tempo e os problemas ocasionados nem sempre são passíveis de solução. Portanto, será primordial:

- Evitar a perda de contas, por meio de um mecanismo seguro contra o roubo de identidade.
- Dispor de meios eficazes para detectar possíveis conexões fraudulentas no caso de credenciais serem roubadas.
- Criar mecanismos para que os usuários legítimos recuperem suas contas.

4 Proteção de dados/uso indevido

Na era digital, os dados podem ser mais valiosos do que o dinheiro; e eles se tornarão ainda mais importantes à medida que o metaverso se tornar *mainstream*. Tecnologias imersivas, como a realidade virtual e a realidade aumentada, oferecem a oportunidade de coletar muito mais informações do que os dispositivos móveis podem gerar. O aumento do número de sensores em tais tecnologias permite correlacionar muitos sinais e diferentes informações, facilitando a solução de problemas que hoje são extremamente difíceis.

> Conforme os limites da Internet se expandem, a superfície de ataque para os crimes cibernéticos cresce também.

Conheça alguns usos potenciais das tecnologias imersivas:

- Detecção precoce de doenças.
- Melhoria no desempenho de esportistas.
- Navegação pelas ruas movimentadas de uma cidade desconhecida, para localizar um restaurante próximo, uma atração turística, o local de um *show* etc.

Se existem muitos dados circulando, é fundamental tomar medidas para protegê-los. O uso indevido de dados capturados por maus atores inseridos no metaverso pode acarretar danos reais às vítimas. Por exemplo: o movimento do corpo e a maneira como uma pessoa fala podem, em alguns casos, ser coletados e analisados para construir pontos de dados e prever preferências e decisões; ao mesmo tempo, essas informações podem ser usadas indevidamente para rotular a orientação sexual ou a afiliação política da vítima de maneira negativa.

À medida que mais desenvolvedores construam sua própria experiência nas plataformas do metaverso, a concessão de acesso ao nível adequado de dados deve ser minuciosamente examinada e ativamente monitorada, evitando assim a coleta ilegal ou o uso indevido dos dados disponibilizados para as plataformas.

O metaverso evolui com rapidez e os líderes de segurança precisam permanecer vigilantes, trabalhando com os diversos *stakeholders* para construir um programa holístico de segurança cibernética. Ao fazer isso, eles inspirarão a confiança de todas as partes interessadas, criando as condições ideais para crescer, inovar e ter sucesso.

Fale com o nosso time

Thammy Marcato
Sócia-diretora de Inovação e Transformação da KPMG no Brasil e co-founder da KPMG e Distrito Leap
tmarcato@kpmg.com.br

Leandro Augusto Marco Antonio
Sócio-líder de Cyber Secutiry & Privacy da KPMG no Brasil e na América do Sul
lantonio@kpmg.com.br

Os serviços descritos neste material, no todo ou em parte, podem não ser permitidos a ser prestados a clientes de auditoria da KPMG e suas afiliadas ou entidades relacionadas

kpmg.com.br

/kpmgbrasil

Projeto gráfico e diagramação: Gaudí Creative Thinking.