Vertigo3d_CANVA

DADOS REAIS REORGANIZADOS

IDENTIDADES SINTÉTICAS: A AMEAÇA DE SEGURANÇA QUE OS SISTEMAS ATUAIS NÃO DETECTAM

A detecção de identidades sintéticas tornou-se um dos maiores desafios da cibersegurança moderna. As ameaças à identidade digital continuam crescendo.

Leonardo Gonzalez (*)

Os deepfakes dominam a cobertura da mídia, os ataques de phishing se tornaram rotina e os casos de profissionais de TI norte-coreanos infiltrados em grandes corporações já não surpreendem ninguém.

Esses casos podem concentrar toda a atenção, mas acredito que deveríamos falar mais sobre outra ameaça à identidade. A ameaça da qual falo é mais sutil, mas extremamente insidiosa. Os agentes maliciosos já utilizam IA para reunir dados públicos e pessoais vazados e construir identidades sintéticas. Refiro-me a pessoas que parecem e agem como pessoas reais porque foram criadas a partir de dados reais, apenas reorganizados em alguém que não existe.

Essas identidades sintéticas representam um problema sério porque os sistemas de detecção de fraude não foram projetados para isso. Precisamos de modelos de IA treinados para reconhecer comportamento humano anômalo e intenção maliciosa.

A urgência é real em todos os lugares, especialmente na América Latina. Segundo a LexisNexis Risk Solutions, a fraude por identidades sintéticas representa cerca de 48% dos incidentes na região, número que reflete tanto a sofisticação dos ataques quanto a lacuna nas defesas atuais. As organizações não podem esperar que isso se normalize globalmente. Precisam agir agora!

Como funcionam as identidades sintéticas e por que elas escapam da detecção tradicional?

As identidades sintéticas são construídas a partir de dados legítimos — endereços reais, históricos profissionais reais, conexões sociais reais — que são misturados e combinados para criar uma personalidade convincente. Cada dado é válido. A combinação é inventada.

Os sistemas de detecção de fraude procuram padrões "ruins", mais precisamente, desvios comportamentais e

Divulgação

Leonardo Gonzalez

> "A fraude por identidades sintéticas representa cerca de 48% dos incidentes na região, número que reflete tanto a sofisticação dos ataques quanto a lacuna nas defesas atuais.

anomalias conhecidos, como por exemplo; informações proibidas, credenciais previamente marcadas, verificações de velocidade. Isso funciona quando os atacantes invasores reutilizam a mesma informação fraudulenta. Mas as identidades sintéticas geralmente não são reutilizadas. Cada uma é criada do zero a partir do enorme volume de dados pessoais que circulam na internet e em bancos de dados de violações de segurança. Quando você consegue identificar uma, o invasor já está construindo a próxima.

Verificação de identidade baseada em comportamento: a abordagem que realmente funciona

Os seres humanos reais têm padrões: como escrevem, quando estão ativos, quais sistemas acessam e em que ordem, como reagem quando algo inesperado acontece. Existe um ritmo na forma como as pessoas trabalham. Poderíamos chamar isso de cadência humana.

As identidades sintéticas, mesmo as mais bem construídas, apresentam falhas. O comportamento parece estranho. Os padrões de acesso não correspondem ao perfil da função. A atividade aparece em horários incomuns. Quando passam por uma verificação de rotina, a resposta parece ensaiada. Não é tão óbvio quanto um deepfake malfeito, mas é muito fácil cair na armadilha.

Modelos de IA treinados em comportamento humano conseguem detectar essas falhas. Não comparando com uma lista de assinaturas maliciosas conhecidas, mas percebendo quando algo simplesmente não corresponde à forma como uma pessoa real age.

Como implementar a detecção de identidades sintéticas na prática

Quando profissionais de segurança proativos desenvolvem funções de segurança, eles as analisam sob dois ângulos: como os clientes irão utilizá-las e como os invasores poderiam explorá-las. Analisar as capacidades pela perspectiva do adversário é o que deve orientar essas decisões.

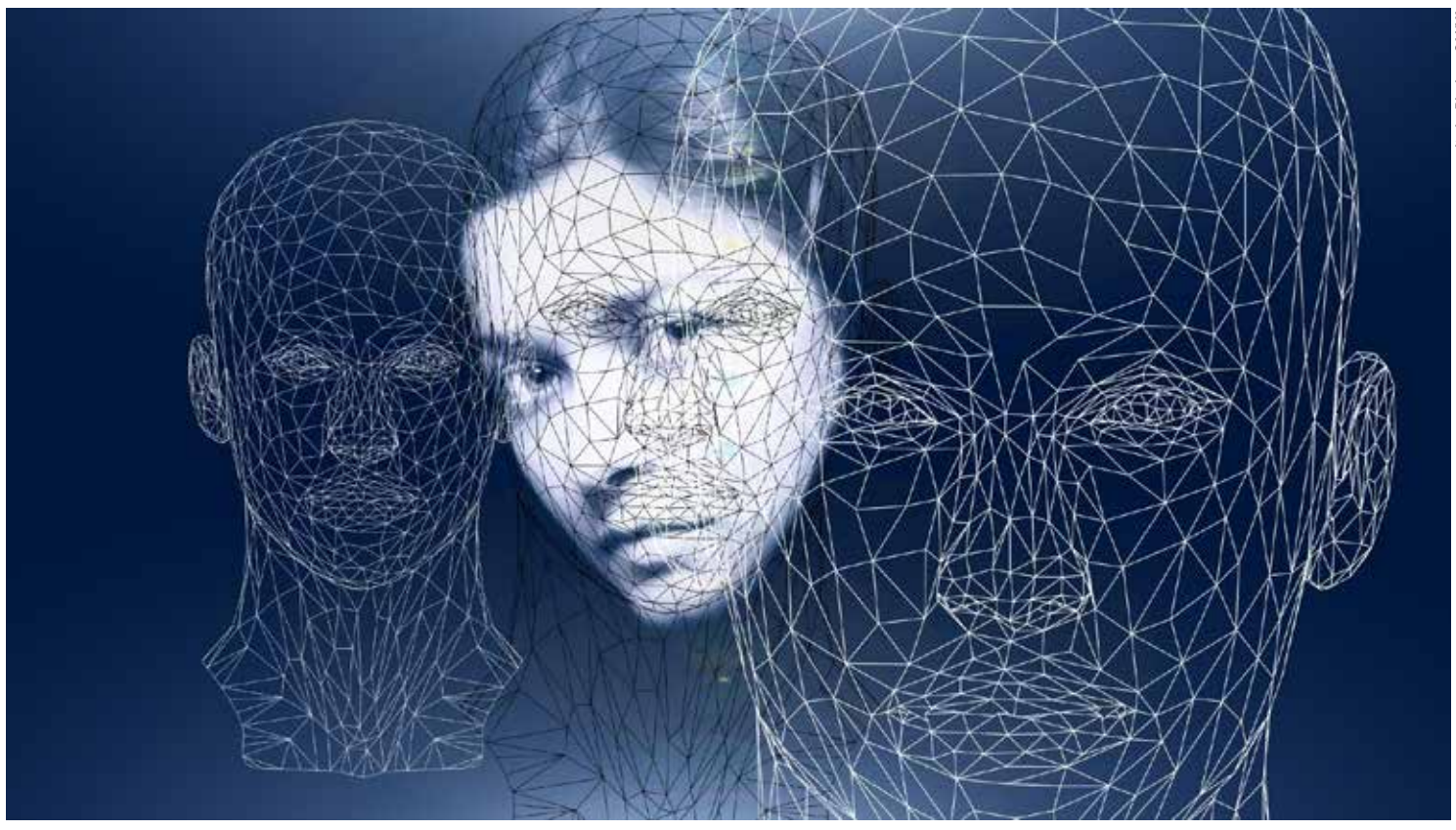
A verificação de identidade exige a mesma abordagem. Precisamos parar de perguntar se uma identidade possui credenciais válidas. Precisamos perguntar se ela se comporta como a pessoa que afirma ser.

A maioria das organizações não está preparada para detectar identidades sintéticas

A maioria ainda depende da autenticação por credenciais e da detecção de fraude baseada em regras. Verificam usuário e senha. Confirmam que se o documento de identidade não está em uma lista negra. Consideram o resultado válido e seguem em frente.

Isso não resiste diante de identidades sintéticas criadas exatamente para passar por esses controles.

Migrar para uma detecção baseada em comportamento exige investimento. Significa repensar completamente como funciona a verificação de identidade e aceitar que credenciais sozinhas não comprovam que alguém seja quem diz ser. É necessário observar como as pessoas se comportam ao longo do tempo. Isso exige mais trabalho no início, mas é uma daquelas situações em que um grama de prevenção vale, no longo prazo, muitos quilos de solução.



gerait_de_Pixabay_CANVA

(*) Especialista em transformação digital, com mais de 25 anos de experiência na indústria de tecnologia. Atualmente lidera a estratégia da Ivanti na América Latina como Diretor Regional, impulsionando a inovação em operações de TI e segurança empresarial.