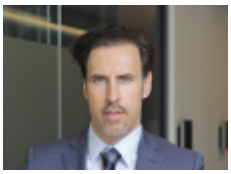
Tomorrow is hackable: o desafio das tecnologias emergentes



Bruno Castro

O avanço tecnológico que tem impulsionado as organizações na era digital também trouxe consigo crescentes ameaças à cibersegurança. Dizer que o amanhã é “hackeável” reflete não apenas uma possibilidade, mas antes, uma realidade iminente que as organizações enfrentam, quer no setor público quer no privado. Já não se trata de uma questão “de”, mas de “quando”.

À medida que nos aproximamos de uma sociedade cada vez mais interconectada, as ciberameaças evoluem em complexidade, sofisticação e rapidez. O ciberespaço, tornou-se um campo de batalha virtual onde organizações e indivíduos lutam contra ameaças persistentes oriundas também de uma comunidade criminosa em crescendo. Um dos desafios fundamentais é a constante adaptação dos cibercriminosos às mais recentes tecnologias de segurança. Quando falamos de cibercrime não falamos em jovens adolescentes *hackers* inexperientes; atualmente, lidamos com grupos criminosos, tecnicamente especializados, experientes e muito organizados, tal como se se tratasse de uma “mafia cibernética” com um modelo de negócio eficaz, rentável, distribuído geograficamente, e sobretudo, com a vantagem “tempo”, todo o tempo do mundo, do seu lado. Atualmente, proteger uma organização implica estar dois passos à frente, estarmos preparados para o inesperado e muitas vezes (se não, quase sempre) em constante corrida contra o tempo.

As tecnologias emergentes, uma categoria onde se inclui a Inteligência Artificial (IA) Generativa, podem igualmente exacerbar os desafios que as organizações enfrentam. A IA, apesar de conferir benefícios significativos, também abre portas para ameaças avançadas ao automatizar e ampliar a superfície dos ataques, tornando-os mais sofisticados e disruptivos. Muitas vezes são pequenos (mas grandes) pormenores, tais como, tornar um email de *phishing* mais credível, leia-se, mais difícil de reconhecer como fraudulento ou malicioso para a vítima. Outros casos, já são mais complexos, como os *deepfakes* – isto é, IA utilizada para criar perfis, vídeos, imagens e áudios falsos de pessoas reais. O facto de qualquer utilizador da Internet conseguir criar conteúdos sintéticos a baixo custo tornou a questão particularmente complexa e sem consensos. Nos últimos anos, as aplicações e ferramentas de IA para a produção de conteúdos falsos multiplicaram-se, tornaram-se demasiado económicas, acessíveis e relativamente fáceis de utilizar. Em simultâneo, a credibilidade dos resultados melhorou de forma considerável, permitindo agora a criação de imagens, ficheiros de som e vídeos, muito difíceis de distinguir do material autêntico. Veio trazer uma nova variável ao cibercrime, ou seja, para além de ter de desconfiar do que está escrito, também terei de passar a desconfiar do que vejo e ouço daqui em diante.

Esta nova variável do cibercrime - *deepfakes* – pode vir a ter o potencial de impactar a reputação de organizações, minar resultados eleitorais, comprometer a estabilidade social e até a segurança nacional de um país, especialmente, no contexto de campanhas de desinformação.

Também os dispositivos IoT (Internet of Things) apresentam novos pontos de entrada para ciberataques. A segurança frágil destes dispositivos pode ser explorada, e é expectável um incremento nos ataques direcionados a dispositivos conectados, explorando naturais vulnerabilidades de segurança numa tendência que é cada vez mais real. A expansão de equipamentos inteligentes, num conceito de *smarthome* ou *smartcity* terá um impacto violento no que respeita a cibersegurança do mundo digital. Teremos de passar a olhar, também, com desconfiança para esta nova evolução digital. É por isso imperativo que as organizações procurem um maior entendimento acerca do impacto efetivo das tecnologias emergentes que adotam e que sejam capazes de reter talento capaz de aplicar essas mesmas tecnologias de forma ética e resiliente.

Enfrentar os desafios da cibersegurança requer uma abordagem holística e integrada. As organizações devem adotar medidas proativas e promover a colaboração entre o setor público e privado para uma maior compreensão sobre as ameaças reais e emergentes, e saber como desenvolver e implementar estratégias eficazes de defesa. Se o amanhã é, de facto, hackeável, será também defensável.

Fundador & CEO da VisionWare. Especialista em Cibersegurança e Análise Forense