Mindset Cibersegurança versus Mindset Cibercrime

dinheirovivo.pt/6198870081/mindset-ciberseguranca-versus-mindset-cibercrime

No vasto campo digital onde se desenrola a batalha incessante entre defesa e ataque, crime e segurança, destacam-se dois *mindsets* completamente opostos: mindset profissional de cibersegurança versus *mindset* cibercrime.

Para entender melhor este contraste, podemos fazer uma analogia com o confronto histórico entre as autoridades e a máfia. Assim como a máfia utiliza estratégias e uma rede altamente sofisticada, em escalada de corrupção para alcançar os seus objetivos, os cibercriminosos aplicam técnicas avançadas e táticas subversivas para invadir, roubar e causar disrupção. Do outro lado temos os profissionais de cibersegurança, que todos os dias têm o desafio de antecipar estas ameaças, prevenir que atinjam o seu objetivo e, quando tal acontece, conter o mesmo e assegurar a normal recuperação.

Os cibercriminosos, tal como a máfia, operam com um conjunto claro de objetivos, nomeadamente, lucro, poder e controlo. *Ransomware*, phishing, fraudes financeiras e roubo de identidade são apenas alguns exemplos de operações conduzidas pelos cibercriminosos para levar a cabo o seu negócio. Isto leva-nos também a uma outra grande diferença – se, por um lado, os cibercriminosos têm um core business, e é esse o seu foco principal, um profissional de cibersegurança tem de lidar com uma série de outras vertentes. Os cibercriminosos tendo um foco específico estão também permanentemente a planear novas táticas “outside the box”; por outro lado, um profissional de cibersegurança, tem de estar sempre preparado para o inesperado e para endereçar todo o tipo de ameaças. De facto, a capacidade de adaptação e inovação ao mundo do cibercrime podemos dizer que é notável – existe a constante procura de novas formas de contornar as medidas de segurança ao demonstrar um nível de criatividade e persistência que faz lembrar histórias da máfia relativamente à sua habilidade, bem conhecida, de se reinventar para escapar à lei.

Um profissional de cibersegurança além da criatividade que também é necessária, requer também que o seu *mindset* contemple a ética e disciplina, valores cruciais para a defesa e proteção de redes e sistemas das contantes e persistentes ciberameaças. Aquilo que os caracteriza, e de forma notável é, acima de tudo, a sua capacidade resiliência. Além do seu profundo conhecimento técnico, do lado da cibersegurança, a abordagem a seguir é tanto proativa como reativa, há que prevenir a ocorrência do ataque, contudo, caso tal aconteça, têm a responsabilidade de reagir perante o mesmo, por vezes, nas piores circunstâncias e em corrida contra o tempo. De facto, este último é sem dúvida um fator em jogo e de grande peso: o tempo. Enquanto um atacante dispõe de tempo de planeamento da estratégia e preparação do ataque, um profissional de cibersegurança, não só não tem tempo, como corre contra o tempo, tendo o objetivo de mitigar um ataque o mais rápido possível, de modo a conter os danos. Adicionalmente,

no ciberespaço o seu cariz sem fronteiras e geografias, impulsiona a difusão do ataque dificultando quer a sua contenção quer a atribuição, ou seja, descobrir a origem do ataque e os seus responsáveis.

Assim como a máfia sempre encontrou novas formas de operar mesmo perante as maiores adversidades, adaptando-se rapidamente às novas tecnologias e contramedidas de cibersegurança, também do lado da cibersegurança, esteve deverá ser o caminho. No panorama do cibercrime observamos ataques cada vez mais sofisticados, altamente personalizados e complexos, em grande parte devido ao suporte de novas tecnologias, como são exemplos a inteligência artificial (IA) e *machine learning* (ML). Do lado da cibersegurança, de quem defende, é vital que também exista esta adaptação às novas tecnologias, e uma certa ousadia e mindset "outside the box". Esta evolução do lado da defesa já acontece – cada vez mais são desenvolvidas e implementadas novas tecnologias de defesa, de IA e ML para detetar e mitigar ameaças, de modo mais eficiente.

Por fim, diria que, uma outra característica importante para quem trabalha em cibersegurança é a humildade, principalmente, perante as adversidades e nos piores cenários, saber pedir ajuda, manter uma comunicação ativa com os outros profissionais envolvidos e também saber aprender com os erros, procurando ser melhor e fazer melhor. No fundo, a batalha entre cibercriminosos e profissionais de cibersegurança não é apenas uma luta técnica, mas é também uma batalha de valores e princípios. E, assim como a máfia não foi erradicada da noite para o dia, a luta contra o cibercrime é um esforço contínuo que requer compromisso, colaboração, resiliência e uma constante vontade de superação, do lado da defesa.

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