Ciberataque AMA: quando a pressa é inimiga da perfeição

digitalinside.pt/ciberataque-ama-quando-a-pressa-e-inimiga-da-perfeicao

É preocupante, especialmente para quem trabalha nesta área há tantos anos, ver a rapidez com que foi descartada a hipótese de acesso ilegítimo a dados. É difícil recordar-me de uma ocasião de recuperação a desastres e resposta a incidentes assente em ciberataques, principalmente, da categoria ransomware, em que foi tão rápida a conclusão de não existir "evidências" de fuga de dados. Digo, especificamente em casos de ransomware, porque este é sem dúvida um dos ataques mais violentos e disruptivos para qualquer organização, um dos mais difíceis em termos de resposta & recuperação, mas também, e principalmente de investigação forense. Este tipo de ciberataque envolve uma intrusão prévia, usurpação de identidade com escalação de privilégios (por regra, ao topo da pirâmide da estrutura de identidade), com posterior acesso ilegítimo aos dados da organização e consequente roubo dos mesmos, onde depois é aplicado algum mecanismo de inacessibilidade – encriptação ou destruição – dos dados para que, de seguida seja então exigido o retorno financeiro através de pedidos de resgate. Assente nesta sequência típica de ações, e face ao nível de acessos – privilegiados em causa – parece-me cada vez mais (no mínimo) questionável, o facto de não existir roubo de dados.

Sabemos que, não existem organizações 100% seguras e livres de serem vítimas de cibercrime. Ninguém está imune ao cibercrime que é nos dias de hoje um modelo negócio altamente maduro, rentável, com profissionais especializados e com vários recursos ao dispor, nomeadamente, skills e tempo. Defendo que, aquilo que as organizações podem, e devem fazer, é gerir o risco de forma adequada ao seu negócio, consoante o nível de maturidade expectável ou exigido para a sua atividade ou posicionamento de mercado. Ainda assim, e apesar de todo o planeamento e governance instituídos numa organização, também não deixo de assumir que a métrica de "todos temos um plano, até um desastre acontecer" é a realidade se nos depara nestas ocasiões. É precisamente nestas alturas que é importante agir e contar com os melhores e mais experientes profissionais, sim, porque ainda acredito que a experiência do "been there, done that", é fundamental para gerir a situação de desastre – onde tudo é volátil e arriscado – para que a recuperação seja o menos penosa possível. É imprudente, adjudicar serviços de apoio "em cima do joelho" motivado pelo carácter de urgência sem existir um rigoroso "fact check". Nesta fase, qualquer organização deve ter a consciência de reconhecer que foi vítima de um ciber desastre, não é algo que só acontece aos outros, e como tal, é fundamental ter a capacidade de "decidir bem" num momento onde todas as variáveis nos parecem sem solução. O saber a quem recorrer nestas situações de crise, face às suas competências, disponibilidade (capacidade de trabalhar em contínuo, dias/noites a fio) e experiência comprovada em situações semelhantes é fundamental para uma recuperação com o menor impacto possível.

Muitas vezes me questionam sobre como funciona a mecânica da operação de resposta a um ciberataque, no fundo, o que se passa no contexto a que chamamos de sala de crise. Não existe uma receita mágica, mas no essencial, baseia-se inicialmente, na implementação – o mais rápido possível – das ações de contenção e anulação do ciberataque, e daí em diante, muitas vezes em simultâneo, tratar do processo de recuperação e higienização dos sistemas comprometidos, que provavelmente, será a fase atual neste caso da AMA. Obviamente que, durante todo o processo, é fundamental o papel da equipa de investigação forense, que deverá providenciar a resposta às três questões fulcrais – "quem?" "quando?" e "como?". Somente depois de termos uma resposta credível a estas questões é que estaremos em condições de retomar a atividade. Estou consciente das regras da equação do tempo *versus* criticidade, em que atividade exige que se recupere rapidamente os serviços face à exigência (muitas vezes) do top management e stakeholders, contudo, a realidade é que, sem se perceber quem está por detrás do ciberataque, qual o método de intrusão utilizado, quem foi o "paciente-zero", ou como (e para onde) é que foi realizada a exfiltração de dados, entre outras informações, é irresponsável a retoma súbita da atividade sob o risco de surgirem outros ciberataques *à posteriori*, geralmente, com maior gravidade (nem que seja impacto mediático e dano reputacional/quebra de confiança na marca/entidade).

Em casos de ciberataques com ransomware, por um lado, o facto de se deixar uma "pegada" para obter o resgate e o respetivo trade off financeiro, abre (muitas vezes) a nossa janela de oportunidade para iniciar o processo de investigação. Perceber quem é o grupo cibercriminoso, o seu *modus operandi*, como funciona o roubo de dados, onde se movimenta na darkweb, e obviamente, qual o método de "comercialização" dos dados, algo que é frequente acontecer – os dados são roubados e depois revendidos a outros grupos criminosos – torna-se um bloco de informação crucial para a investigação e até, ação criminal posterior. Aproveito para reforçar que qualquer "acordo" com o grupo cibercriminoso, nomeadamente, o pagamento para a recuperação ou não-divulgação de dados, vale apenas pela "palavra de um criminoso", ou seja, nada. Sou muito claro aqui: por maior impacto que exista no ciberataque em questão, o alimentar financeiramente uma rede criminosa, jamais pode ser uma opção válida.

Esta é sem dúvida, uma situação complexa tecnicamente, muito exigente mental e fisicamente, onde a pressão por decisões arriscadas, é justamente o panorama ideal para se cometer erros que se podem tornar ainda mais catastróficos, e como tal, as conclusões e decisões não podem ser precipitadas. Ainda não há muito tempo, tivemos um exemplo nacional em que a entidade lesada veio publicamente dizer que o ciberataque teria sido contido sem comprometimento dos dados pessoais, sendo que, passado pouco tempo, veio a descobrir-se que, afinal os cibercriminosos tinham divulgado os dados roubados, massivamente, na dark web. Será que não aprendemos nada com os erros de comunicação do passado? A pressa e a precipitação em prestar afirmações e conclusões dúbias em situações tão voláteis como esta, podem ser, efetivamente, inimigas da perfeição e do bom senso.

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