Ransomware e o perigo de negociar com criminosos

digitalinside.sapo.pt/ransomware-e-o-perigo-de-negociar-com-criminosos

Bruno Castro

O mais recente relatório da Sophos sobre o estado do ransomware em 2025 revela uma aparente evolução na forma como as organizações lidam com ataques de ransomware. Com uma queda de 50% no pagamento médio de resgates e mais de metade das empresas a conseguirem negociar montantes inferiores ao inicialmente exigido, poderá haver a tentação de interpretar estes dados como um sinal positivo. No entanto, esta narrativa esconde um risco estratégico perigoso: a normalização do pagamento de resgates como parte da resposta ao incidente.

***Spoiler alert:* pagar ou negociar com criminosos não é uma estratégia – é uma cedência que perpetua o ciclo de ataques**

O facto de 71% das reduções no valor do resgate se deverem a processos de negociação não é uma vitória. É uma prova de que os atacantes já contam com esse jogo psicológico e orçamental. Eles sabem que ao pedirem somas exorbitantes, haverá margem para "ceder", no entanto conseguem manter o lucro e ainda reforçam o modelo de negócio criminoso. Cada euro pago, mesmo que abaixo do pedido inicial, alimenta esta economia paralela.

Outro argumento recorrente é que pagar o resgate permite recuperar os dados mais rapidamente. Mas a realidade é incerta: não há garantias de que os dados serão totalmente restaurados, de que não foram copiados ou vendidos, ou que os sistemas não voltarão a ser comprometidos. Vários casos documentados demonstram que muitas organizações são atacadas novamente após pagar – algumas pela mesma ameaça, outras por grupos diferentes que sabem que "pagam bem" ou estão abertas à negociação.

Em alguns países, pagar resgates a grupos ligados a organizações terroristas ou sancionadas pode ter implicações legais. Mais do que isso, há uma questão ética incontornável: ao pagar, estamos a financiar diretamente o crime organizado e a contribuir para a sua sustentabilidade.

A verdadeira maturidade na resposta a incidentes não está na negociação bem-sucedida, mas na preparação que evita a necessidade de o fazer. O que realmente deve ser celebrado neste relatório não é a redução nos valores dos resgates pagos, mas sim o facto de que as organizações estão mais eficazes a recuperar sem pagar. Segundo os dados disponibilizados, excluindo qualquer resgate, o custo médio de recuperação de um ataque de ransomware desceu 44% num ano, passando de 2,73 milhões de dólares em 2024 para 1,53 milhões em 2025. Esta redução significativa demonstra que as empresas estão a investir em medidas preventivas e planos de resposta mais eficazes, permitindo-lhes mitigar os danos com maior eficácia.

Adicionalmente, a velocidade de recuperação também melhorou substancialmente: em 2025, 53% das organizações conseguiram recuperar totalmente em apenas uma semana, comparado com apenas 35% em 2024. Estes são os verdadeiros indicadores de maturidade na ciberdefesa. Revelam que a preparação, a implementação de backups seguros, a segmentação de redes e a formação contínua das equipas estão a produzir resultados concretos.

Como líderes de cibersegurança, temos a obrigação de transmitir uma mensagem clara: não se negocia com cibercriminosos. Em vez de focarmos os nossos esforços devem ser focados em reforçar a capacidade de resistir e recuperar rapidamente, sem ceder a chantagens. Devemos preparar as organizações para resistir, responder e recuperar sem alimentar o ciclo de extorsão. Devemos trabalhar com parceiros, autoridades e especialistas para criar uma frente comum que reduza a rentabilidade deste tipo de ataque. Só assim conseguiremos quebrar o ciclo do ransomware e reduzir, de forma sustentada, o impacto deste tipo de ameaça.