Ransomware: o dinheiro ou os dados?

dinheirovivo.pt/opiniao/ransomware-o-dinheiro-ou-os-dados-13411308.html

3 de março de 2021

A segunda vaga de Covid-19 voltou a fechar-nos em casa, com aulas à distância e em teletrabalho, deixando a descoberto as fragilidades digitais que ainda persistem na grande maioria das organizações e empresas portuguesas. Mais uma vez, voltámos a estar na mira dos grupos cibercriminosos, que se aproveitam do facto de existir um número muito maior de potenciais alvos para desenvolverem ciberataques, com enorme taxa de sucesso e com enorme impacto reputacional e financeiro.

Só nas últimas semanas, na VisionWare, registámos um aumento exponencial dos pedidos de investigação forense, associados a um volume de ataques bem-sucedidos de ransomware. Este tipo de ataque, apesar de ter alguns anos de atividade na comunidade de cibercrime, tem vindo a evoluir no seu método de infeção e posterior "chantagem" financeira. Baseia-se num processo de infeção, (cada vez mais) efetuado através de ataques prévios de *phishing* (ou *spear-phishing*) para a "injeção" de malware na vítima, com a nuance de implicar ações de roubo e encriptação de informação e, posteriormente, de chantagem, que podem envolver vários pedidos de resgate (*ransom*), quer seja para devolver a "chave" de acesso à informação encriptada ou para não a divulgar publicamente.

Por princípio, e tendo em consideração que se trata de "crime", a nossa recomendação é clara: não devem ser pagos os pedidos de resgate. Primeiro, porque o resgate pago financia redes criminosas; segundo, porque o pagamento do resgate não garante que o grupo cibercriminoso cumpra com o acordo e devolva a "chave de desencriptação" para posterior acesso à informação. Por fim, e mesmo que isso aconteça, não existe garantia de

que esta informação esteja segura e não venha, mais tarde, a ser utilizada num outro crime, ou que não venha a existir novo pedido de resgate - assente em chantagem - para, por exemplo, não divulgação da informação roubada.

Tipicamente, e cada vez mais, face a esta pandemia também cibernauta, as consequências de ciberataques têm vindo a ter um impacto cada vez maior, o que se deve, essencialmente, à necessidade de nos vermos obrigados a "viver" na Internet. No caso de ataques como o ransomware, o impacto é ainda mais gravoso, visto que, para além de implicar uma interrupção do serviço da organização - através da imposição da inacessibilidade à informação -, poderá ainda colocar em causa a exposição pública de informação confidencial ou sensível. Este tipo de ataque coloca a organização completamente refém do grupo cibercriminoso, o que poderá levar essa mesma organização a uma situação financeira muito difícil, afetando, por exemplo, a sua reputação, a dos seus parceiros, e até dos seus colaboradores, de forma muitas vezes irreparável.

Para que se compreenda melhor o impacto de um ciberataque, trago hoje o exemplo de um caso ocorrido recentemente nos Estados Unidos e que me chocou particularmente. Conforme reportado pela Israel Defense, o sistema de fornecimento de água da cidade de Oldsmar foi vítima de um ciberataque na sua vertente mais maléfica - ciberterrorismo - e que, caso tivesse sido bem sucedido, poderia ter provocado o envenenamento em massa da população da região. Alguém, ainda por identificar, acedeu aos computadores daquela infraestrutura e fez aumentar a quantidade de hidróxido de sódio, um químico utilizado para controlo de acidez da água, mas que em doses excessivas pode causar problemas de pele, queda de cabelo e até a morte (no caso de ser ingerido). Felizmente, um trabalhador identificou a concentração anormal daquele químico e conseguiu impedir o pior. Ainda assim, e até pelo desconhecimento do processo de intrusão, o sistema na sua globalidade teve de ser temporariamente interrompido até à recuperação do ataque e para ação de melhoria de cibersegurança.

Este caso alerta para um aspeto particularmente perigoso do cibercrime: quando bem-sucedido, as suas consequências não ficam apenas no plano digital e podem representar um risco real com graves repercussões para a sociedade, os seus cidadãos e empresas ou organizações, até mesmo a um nível mundial.

É por isto que insisto que a cibersegurança é imprescindível face a esta pandemia cibernética. O mundo nunca mais será o mesmo: a presença na Internet passará a ser um pilar base da nossa sociedade e, consequentemente, das empresas, organizações, estados e cidadãos.

Mais do que remediar, é necessário prevenir, garantindo que temos estruturas resilientes, no que respeita à cibersegurança. Só desta forma estaremos aptos a viver de forma segura e a gerir este novo nível de exposição.

CEO da Visionware