MINISTÉRIO DA TRANSPARÊNCIA E CONTROLADORIA-GERAL DA UNIÃO
DIRETORIA DE GESTÃO INTERNA

PEDIDO DE ESCLARECIMENTO Nº 07 – PE Nº 06/2018

Segue abaixo a resposta ao Pedido Esclarecimento nº 07 – PE nº 06/2018:

QUESTIONAMENTO 1:

Em relação ao Item Item 19.2.5.5. - Quanto a ataques à camada de aplicação, para os protocolos HTTP e DNS, a solução deve manter uma lista dinâmica de endereços IP bloqueados. Seguem nossas considerações:

a) Por trabalharem com coleta de amostragem de tráfego (flow) dos roteadores dos clientes em modo out-of-path, e por isso não possuem visibilidade de todo o tráfego, as soluções em nuvem possuem como escopo a detecção de ataques que provoquem variações significativas no perfil habitual de tráfego (baseline) em quantidade de bits ou pacotes por segundo, e/ou que atinjam os thresholds definidos pelo cliente para geração de alertas.

b) O escopo de detecção e mitigação de ataques de aplicação e/ou criptografados contempla a verificação da conformidade dos pacotes com a RFC dos protocolos.

c) Isto significa que não é possível a detecção de ataques com tráfego criptografado e/ou voltados para a aplicação e cujo conteúdo malicioso esteja no payload dos pacotes.

Com base nos pontos citados acima, entendemos que de acordo com a necessidade da contratante, será necessário contemplar a disponibilização de um appliance a ser instalado inline na rede a ser protegida. Nosso entendimento está correto?

RESPOSTA 1:

Não, o entendimento não está correto.

A CONTRATADA deve utilizar os meios necessários para atender os requisitos estabelecidos pelo item 19.2.5.5: “Quanto a ataques à camada de aplicação, para os protocolos HTTP e DNS, a solução deve manter uma lista dinâmica de endereços IP bloqueados.”. A utilização do *appliance inline* dependerá da arquitetura provida pela empresa contratada.

QUESTIONAMENTO 2:

Referente ao exigido no item 19.2.6 – “A CONTRATADA deve possuir, no mínimo, 2 (dois) centros de limpeza, cada um com capacidade de mitigação de ataques. Dos centros de limpeza, pelo menos um deverá estar em território nacional e pelo um deverá estar no exterior. Para a mitigação dos ataques de origem no território brasileiro não será permitido o encaminhamento do tráfego para limpeza fora do território brasileiro.”

Entendemos que não faz diferença para a Contratante a obrigatoriedade da instalação de plataformas de limpeza fora do território nacional já que todo o tráfego de ataques será mitigado na rede da Contratada não tendo impacto na qualidade do serviço prestado.

Entendemos ainda que o impacto seria se a contratada só tivesse plataformas internacionais, fazendo com que o tráfego gerado em território nacional fosse desviado para fora do Brasil gerando maior latência além de questões relacionadas ao Marco Civil sobre este tema.

Diante disso, sugerimos a retirada da obrigatoriedade de a Contratada possuir plataformas de limpeza de tráfego instaladas fora do território nacional.

Nossa sugestão será acatada?

RESPOSTA 2:

Não, a sugestão não será acatada.

O centro de limpeza nacional será responsável por mitigar os ataques oriundos do Brasil enquanto o centro de limpeza fora do país se responsabilizará por mitigar os ataques de origem internacional.

QUESTIONAMENTO 3:

Item 19.2.7 – "A CONTRATADA deverá prover o serviço de mitigação sem limitação de duração, volume de tráfego, quantidade de pacotes, ataques nacionais ou internacionais, quantidade de eventos, requisições por segundo, intervalos entre os ataques."

Entendemos que não deve haver variações no valor da mensalidade do serviço por conta de serviços adicionais prestados.

Porém, é importante esclarecer que toda plataforma de serviços, independentemente do provedor da tecnologia, não possui capacidades infinita de mitigação.

Neste caso, seria sugerimos que a Contratante defina a capacidade esperada de mitigação de ataques (em *Gbps*) para que todos os provedores estejam balizados pelos mesmos critérios e a contratante tenha clareza no escopo do serviço prestado. Nossa solicitação será acatada?

RESPOSTA 3:

Não, a sugestão não será acatada.

Não é possível determinar o volume ou tráfego de ataque que a CONTRATADA vai sofrer.

QUESTIONAMENTO 4:

Item 15. DAS CONDIÇÕES DE RETIRADA DA NOTA DE EMPENHO, DAS ASSINATURAS E VIGÊNCIAS DA ATA DE REGISTRO DE PREÇOS E DO CONTRATO

15.2. O não comparecimento da licitante vencedora, dentro do prazo de 5 (cinco) dias úteis, após regularmente convocada para assinatura da Ata de Registro de Preços, retirada da Nota de Empenho e/ou assinatura do Termo Contratual, ensejará a aplicação de multa de até 10% (dez por cento) sobre o valor total da proposta ou lance final ofertado, devidamente atualizado

Neste caso, solicitamos que altere este item, pois os procuradores não residem na mesma cidade, o que dificulta o comparecimento ao órgão. Sugerimos que o contrato seja disponibilizado via e-mail ou até mesmo entregue no endereço da empresa vencedora, afim de seguirmos com os trâmites de assinatura.

Solicitamos ainda um prazo mínimo de 10 dias úteis para assinatura do contrato e da Ata de Registro de Preço.

Nossa solicitação será acatada?

RESPOSTA 4:

Em relação ao prazo para assinatura da ata e do contrato, informo que serão assinados eletronicamente, no Sistema Eletrônico de Informações (SEI), após o cadastro dos representantes legais da empresa. Porém deverá ser observado o prazo contido nos itens 15.2 e 15.3.