QUESTIONAMENTO | PREGÃO PRESENCIAL 003/2022 | ALPB

cpl alpb <cpl.alpb@gmail.com> 30 de agosto de 2022 16:19
Para: Lucas Silvino Da Silva <lucas.silvino@oi.net.br>

Prezado Lucas Silvino,

Boa tarde!

Seguem respostas aos questionamentos formulados sobre o edital do Pregão Presencial nº 03/2022 da ALPB:

1. **DO TEMPO DE MITIGAÇÃO PARA OS CIRCUITOS DE 500Mbps**

O TERMO DE REFERÊNCIA, define em seu item **5.4.3.3. PROTEÇÃO CONTRA-ATAQUES DoS (Denial of Service) e DDoS (Distributed Denial of Service)**, para o circuito de 500Mbps, que a mitigação dos ataques do DoS e DDoS deverá ocorrer em até 30 minutos quando descreve:

> *"A CONTRATADA deverá realizar a mitigação dos principais tipos de ataques conhecidos em até 30 minutos (após o trafego ter sido identificado anunciado e reconhecido pela CONTRATADA e autorizado pela CONTRATANTE)."*

O TERMO DE REFERÊNCIA, define em seu item **5.4.3.3. PROTEÇÃO CONTRA-ATAQUES DoS (Denial of Service) e DDoS (Distributed Denial of Service)** também define que:

> *"Em casos de ataques não detectados pela solução, quando identificados pela CONTRATANTE, deverão ser mitigados imediatamente pela CONTRATADA após a abertura."*

Destaca-se que, a detecção é realizada através do monitoramento dos fluxos dos dados e estes analisados por uma plataforma para a correlação de eventos, rastreamento e coleta de estatísticas.

Quando um comportamento anormal é detectado, podendo este ser uma condição de ataque, existe a necessidade da CONTRATADA entrar em contato com a CONTRATANTE, para investigar a condição é de ataque ou não. Ou seja, em alguns casos CONTRATANTE está realizando algum evento pontual em sua rede o qual possa desencadear um comportamento diferente da base line do cliente (ex: época de matrículas em acessos de escolas/faculdades).

Assim, existe a necessidade da CONTRATADA (após o alerta associado a um possível ataque), avaliar se existe algum evento na rede que possa estar levando esta condição. Após esta análise, a equipe SoC da CONTRATADA entre em contato com o cliente para validar a condição ou não de ataque (conforme detalhado acima).

Desta forma, estamos entendendo que a CONTRATADA estará atendendo ao edital oferendo um serviço de proteção contra-ataques do tipo DoS e/ou DDoS aonde os SLA de mitigação estejam em conformidade com os tempos de Detecção Proativa, Autorização e Início da Mitigação conforme abaixo:

- Tempo de Detecção Proativa: tempo entre o primeiro alerta associado a um ataque até que o SOC avalie a incidência como possível ataque e tente contato com o cliente. Com SLA de 15 minutos.
- Tempo de Autorização: tempo necessário para o cliente autorizar a mitigação do ataque, desde solicitação até sua autorização. Este período depende do cliente, logo não é considerado como medida de qualidade do serviço.
- Início da Mitigação: Até 15 minutos após autorização do cliente

Está correto nosso entendimento?

R- A contratada deve entrar em contato e relatar ao contratante até 30mim após o início do ataque e fazer o bloqueio necessário até 30mim após a autorização.

2. **DO TEMPO DE MITIGAÇÃO PARA OS CIRCUITOS DE 300Mbps**

O TERMO DE REFERÊNCIA, define em seu item 5.5.3.3. PROTEÇÃO CONTRA-ATAQUES DoS (Denial of Service) e DDoS (Distributed Denial of Service), para o circuito de 300Mbps, que a mitigação dos ataques do DoS e DDoS deverá ocorrer em até 15 minutos quando descreve:

> *"A CONTRATADA deverá realizar a mitigação dos principais tipos de ataques Conhecidos em até 15 minutos (após o trafego ter sido identificado anunciado e reconhecido pela CONTRATADA ou pela CONTRATANTE)."*

O TERMO DE REFERÊNCIA, define em seu item 5.5.3.3. PROTEÇÃO CONTRA-ATAQUES DoS (Denial of Service) e DDoS (Distributed Denial of Service) também define que:

> *"A contratada deverá comunicar de forma imediata a ALPB sempre que um ataque de Negação de Serviço for detectado."*

Destaca-se que, a detecção é realizada através do monitoramento dos fluxos dos dados e estes analisados por uma plataforma para a correlação de eventos, rastreamento e coleta de estatísticas.

Quando um comportamento anormal é detectado, podendo este ser uma condição de ataque, existe a necessidade da CONTRATADA entrar em contato com a CONTRATANTE, para investigar a condição é de ataque ou não. Ou seja, em alguns casos CONTRATANTE está realizando algum evento pontual em sua rede o qual possa desencadear um comportamento diferente da base line do cliente (ex: época de matrículas em acessos de escolas/faculdades).

Assim, existe a necessidade da CONTRATADA (após o alerta associado a um possível ataque), avaliar se existe algum evento na rede que possa estar levando esta condição. Após esta análise, a equipe SoC da CONTRATADA entre em contato com o cliente para validar a condição ou não de ataque (conforme detalhado acima).

Desta forma, estamos entendendo que a CONTRATADA estará atendendo ao edital oferendo um serviço de proteção contra-ataques do tipo DoS e/ou DDoS aonde os SLA de mitigação estejam em conformidade com os tempos de Detecção Proativa, Autorização e Início da Mitigação conforme abaixo:

- Tempo de Detecção Proativa: tempo entre o primeiro alerta associado a um ataque até que o SOC avalie a incidência como possível ataque e tente contato com o cliente. Com SLA de 15 minutos.
- Tempo de Autorização: tempo necessário para o cliente autorizar a mitigação do ataque, desde solicitação até sua autorização. Este período depende do cliente, logo não é considerado como medida de qualidade do serviço.
- Início da Mitigação: Até 15 minutos após autorização do cliente

Está correto nosso entendimento?

R- A contratada deve entrar em contato e relatar ao contratante até 30mim após o início do ataque e fazer o bloqueio necessário até 30mim após a autorização.

3. **DOS RELATÓRIOS E DASHBOARD PARA OS CIRCUITOS DE 300Mbps**

O TERMO DE REFERÊNCIA, define em seu item **5.5.3.3. PROTEÇÃO CONTRA-ATAQUES DoS (Denial of Service) e DDoS (Distributed Denial of Service),** para o circuito de 300Mbps que:

> *"A CONTRATADA deverá disponibilizar console com dashboards e relatórios que permitam o acompanhamento em tempo real do uso dos links e do serviço de mitigação de ataques de negação de serviço para, no mínimo, 05 (cinco) usuários, contendo endereços IP de origem e destino das conexões, protocolo, portas de origem e destino, e consumo de banda."*

Estamos entendendo que a CONTRATADA estará atendendo ao edital oferendo um serviço de proteção contra-ataques do tipo DoS e/ou DDoS disponibilizando um portal com uma Solução de Gerência de Anti-DDoS a qual irá entregar uma visualização de informações on-line (em intervalos de 5 minutos e de forma gráfica) da rede e com os seguintes itens para cada um dos elementos monitorados:

- Tipo de ataque, horário de início e fim;
- Volume de tráfego bloqueado e não bloqueado;
- Origem de ataques com identificação do endereço IP e porta de origem;
- Destino de ataques, com identificação do endereço IP e porta de destino.
- Dashboards executivos com visão sumarizadas de indicadores de Anti-DDoS;

Está correto nosso entendimento?

R- Além das informações listadas na pergunta, também devem ser informados o uso do link com a informação de tráfego total de download e de upload.

4. **DO PRAZO DE INSTALAÇÃO:**

O **TERMO DE REFERÊNCIA**, define em seu item 6.2 o prazo de instalação quando descreve:

> *6.2. PRAZO PARA INSTALAÇÃO, ATIVAÇÃO, CONFIGURAÇÃO E IMPLANTAÇÃO.*
>
> *"O prazo para instalação, ativação, configuração e implantação do serviço será de 60 (Sessenta) dias corridos contados a partir da emissão da OIS – Ordem de Inicio do Serviço pela ALPB."*

A **MINUTA CONTRATUAL**, define em seu item 6.1 o prazo de instalação quando descreve:

> *" CLÁUSULA SEXTA - PRAZO PARA INSTALAÇÃO, ATIVAÇÃO, CONFIGURAÇÃO E IMPLANTAÇÃO."*
>
> *"6.1. O prazo para instalação, ativação, configuração e implantação do serviço será de 30 (Trinta) dias corridos contados a partir da emissão da OIS – Ordem de Inicio do Serviço pela ALPB."*

Entendemos que o prazo a ser considerado seja o de *60 (Sessenta) dias corridos*, **descrito no TERMO DE REFERÊNCIA**.

Correto nosso entendimento?

R- Correto o entendimento de 60 dias corridos.

5. **DO PRAZO DE INSTALAÇÃO – questionamento II**

Ainda com relação ao prazo de instalação, destacamos que a ativação do Serviço Anti-DDoS necessita ser tratada entre as partes CONTRATADA e CONTRATANTE. Ou seja, existe a necessidade de um **Detalhamento Técnico**, que deve ser avaliado entre as partes e que será tratada após a ativação dos Links de Aceso-Web. Assim, o prazo de ativação do serviço de proteção contra-ataques do tipo DoS e/ou DDoS não está incluso no prazo de ativação dos links físicos. Abaixo alguns exemplos do levantamento dos itens técnicos a serem tratados entre as partes:

- Endereços de IPs, Portas TCP/UDP, Serviços (HTTP, HTTPS, SIP, VÍDEO, etc) a serem protegidos;
- Inventário dos Equipamentos a serem protegidos (Marca, Modelo, Versão de Software, etc).
- Responsáveis da ALPB que serão acionados durante possíveis ataques, que poderão acionar a Equipe de Segurança da CONTRATADA, que poderão alterar os nomes dos componentes da lista de responsáveis da ALPB;

Está correto nosso entendimento?

R- Sim o prazo para instalação do Serviço Anti-DDoS pode ser estendido, de acordo com a contratante, levando em consideração todas as necessidades de acertos e informações repassadas pela contratante.

Atenciosamente,

CPL_ALPB

[Texto das mensagens anteriores oculto]