



cpl alpb <cpl.alpb@gmail.com>

QUESTIONAMENTO | PREGÃO PRESENCIAL 003/2022 | ALPB

Lucas Silvino Da Silva <lucas.silvino@oi.net.br>
Para: cpl alpb <cpl.alpb@gmail.com>

12 de agosto de 2022 21:22

JOÃO PESSOA/PB, 12 DE AGOSTO DE 2022.**À ASSEMBLEIA LEGISLATIVA DA PARAÍBA -ALPB****REF.: PREGÃO PRESENCIAL Nº 003/2022****ASSUNTO: SOLICITAÇÃO DE ESCLARECIMENTO.**

Prezado pregoeiro,

A OI S/A, em recuperação judicial, CNPJ nº 76.535.764/0001-43, sediada na Rua do Lavradio, 71, Centro, 2º andar – sala 201/801, Rio de Janeiro/RJ, CEP: 23.230-070, doravante denominada “Oi”, vem, por intermédio de seu representante legal vem, respeitosamente apresentar seus comentários e/ou questionamentos relativos ao PREGÃO PRESENCIAL Nº 003/2022, EM REFERÊNCIA.

1. DO APPLIANCE DE SEGURANÇA (PORTAS LAN)**a) Página, 13, item 5.3.1.12. - Possuir no mínimo 8 (oito) interfaces Lan Gigabit 10/100/1000 SFP com leds indicativos de atividade;**

Entendemos que para a porta SFP haja uma conexão entre a rede seja por portas elétricas ou portas de fibra, está correto nosso entendimento ? Se sim, favor qual tipo SFP devemos considerar?

b) Página, 13, item 5.3.1.13. Possuir no mínimo 8 (oito) interfaces Lan 10G Ethernet SFP+ com leds indicativos de atividade;

Entendemos que para a porta SFP+ haja uma conexão entre a rede seja por portas de fibra, está correto nosso entendimento ? Se sim, favor qual tipo SFP+, no caso multimodo ou monomodo devemos considerar?

2. DAS CARACTERÍSTICAS TÉCNICAS**a) O TERMO DE REFERÊNCIA, define em seu item 5.4.3.3, página 20, que a mitigação dos ataques do DoS e DDoS deverá ocorrer em até 10 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).”

“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 oferecendo 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?

3. DO PRAZO DE INSTALAÇÃO.

a) O TERMO DE REFERÊNCIA, define em seu item 6.2, página 28, 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 30 (Trinta) dias corridos contados a partir da emissão da OIS – Ordem de Início do Serviço pela ALPB.”

Destaca-se 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 Acesso-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?

Obrigado,
Abraço.

Enviado via iPhone

Atenciosamente,
LUCAS SILVINO DA SILVA
Executivo de Negócios

Esta mensagem, incluindo seus anexos, pode conter informações privilegiadas e/ou de caráter confidencial, não podendo ser retransmitida sem autorização do remetente. Se você não é o destinatário ou pessoa autorizada a recebê-la, informamos que o seu uso, divulgação, cópia ou arquivamento são proibidos. Portanto, se você recebeu esta mensagem por engano, por favor, nos informe respondendo imediatamente a este e-mail e em seguida apague-a.



cpl alpb <cpl.alpb@gmail.com>

QUESTIONAMENTO | PREGÃO PRESENCIAL 003/2022 | ALPB

cpl alpb <cpl.alpb@gmail.com>

17 de agosto de 2022 10:19

Para: Lucas Silvino Da Silva <lucas.silvino@oi.net.br>

Prezado Lucas,

Bom dia!

Seguem respostas aos questionamentos formulados em face do Edital do Pregão Presencial nº 03.2022 da ALPB.

1. DO APPLIANCE DE SEGURANÇA (PORTAS LAN)**a) Página, 13, item 5.3.1.12. - Possuir no mínimo 8 (oito) interfaces Lan Gigabit 10/100/1000 SFP com leds indicativos de atividade;**

Entendemos que para a porta SFP haja uma conexão entre a rede seja por portas elétricas ou portas de fibra, está correto nosso entendimento ? Se sim, favor qual tipo SFP devemos considerar?

R- devem ser consideradas conexoes por fibra otica multimodo.

b) Página, 13, item 5.3.1.13. Possuir no mínimo 8 (oito) interfaces Lan 10G Ethernet SFP+ com leds indicativos de atividade;

Entendemos que para a porta SFP+ haja uma conexão entre a rede seja por portas de fibra, está correto nosso entendimento ? Se sim, favor qual tipo SFP+, no caso multimodo ou monomodo devemos considerar?

R- devem ser consideradas conexoes por fibra otica multimodo

2. DAS CARACTERÍSTICAS TÉCNICAS**a) O TERMO DE REFERÊNCIA, define em seu item 5.4.3.3, página 20, que a mitigação dos ataques do DoS e DDoS deverá ocorrer em até 10 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).”

“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 oferecendo 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- sim esta correto o entendimento

3. DO PRAZO DE INSTALAÇÃO.

a) O TERMO DE REFERÊNCIA, define em seu item 6.2, página 28, 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 30 (Trinta) dias corridos contados a partir da emissão da OIS – Ordem de Início do Serviço pela ALPB.”

Destaca-se 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 Acesso-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- Para esse caso específico pode ser estendido esse prazo.

Atenciosamente,

CPL-ALPB

[Texto das mensagens anteriores oculto]

[Texto das mensagens anteriores oculto]