ExpressoLivre - ExpressoMail

Enviado por:	"Bruno Pereira de Alcantara" <bruno.alcantara@cbtu.gov.br>
De:	bruno.alcantara@cbtu.gov.br
Para:	"'Paulo Cesar Barbosa de Moraes Junior'" <pmoraes@cbtu.gov.br>
Com Cópia:	"'Mayara Suzart Gomes'" <mayara@cbtu.gov.br>, "'Reginaldo Oliveira'" <reginaldooliveira@cbtu.gov.br>, "'GETIN - Gerencia TÃ©cnica de Tecnologia da InformaÃ§Ã£o e ComunicaÃ§Ã£o'" <getin@cbtu.gov.br>, "'Gerencia Geral de LicitaÃ§Ã£o'" <galic@cbtu.gov.br>
Data:	01/07/2025 13:26
Assunto:	RES: Fw: SOLICITAÇÃO DE ESCLARECIMENTO - PREGÃO ELETRONICO 90005/2025 - COMPANHIA BRASILEIRA DE TRENS URBANOS
Anexos:	image001.png (20 KB)

Segue resposta para os questionamentos:

Questionamento 1:

Entendemos que a solução deve implementar mecanismos capazes de detectar e mitigar ataques que façam o uso não autorizado de recursos de rede, automaticamente, tanto para IPv4 e IPv6.
Nosso entendimento está correto?

Resposta Questionamento 1:

Sim, o entendimento está correto. Algumas especificações.

- Capacidade de Mitigação (em Gbps) = 0,3 (volume de tráfego máximo por ataque)

- Existência de atuação automática = SIM (Monitoração Proativa) O Security Operations Center (SOC) deverá realizar a monitoração proativa do nosso range de IP. A ferramenta de detecção de alarmes de negação de serviços possibilita ao SOC uma visão ampla dos alarmes de negação de serviço que são detectados com destino a nossa rede. O SOC deverá atuar e nos notificar.

- Quais camadas do modelo OSI são contempladas na proteção = camadas compatíveis com as identificações dos ataques relacionados abaixo.

- Tipos de ataques cobertos (volumétricos, aplicação, etc.) = Detecção de tráfego suspeito: deverá possuir sistema com inteligência para identificar abusos no uso da rede, principalmente em termos de IP Scan, DDoS e IP Flood. Não haverá monitoramento em camada de aplicação. O sistema deverá registrar as ocorrências e exibi-las em relatórios;

Questionamento 2:
Entendemos que a solução de proteção contra-ataques de negação de serviços deve ser disponibilizada no backbone da CONTRATADA, não sendo permitida a subcontratação da mesma, ou seja, para que a integridade dos dados e informações trafegadas não sejam comprometidas, não será permitido que a CONTRATADA realize o redirecionamento do tráfego para infraestruturas de terceiros para que estes realizem a mitigação dos ataques e não será aceito bloqueio de ataques de DOS e DDOS por ACLs em roteadores de bordas da contratada.
Nosso entendimento está correto? Caso o entendimento esteja correto, as licitantes deverão comprovar que possuem infraestrutura própria de proteção contra ataques de negação de serviços?

Resposta Questionamento 2:

Não será permitido o redirecionamento do tráfego para terceiros para fins de mitigação dos ataques, a fim de garantir a integridade e a confidencialidade das informações trafegadas. Não será permitido a subcontratação de serviço de SOC. A licitante deverá ter serviço próprio.
Não será admitido o uso de ACLS (Access Control Lists) em roteadores de borda como única ou principal estratégia de mitigação.
Sim, a licitante deverá comprovar na sua proposta técnica que possui infraestrutura própria de SOC. Poderá comprovar por meio de documentação técnica, certificações, declarações do fabricante, topologias de rede, ou outros documentos que comprovem a aderência aos requisitos estabelecidos no edital.

Atte.;

Bruno de Alcantara

Gerente Tecnologia da Informação e Comunicação
Cia Brasileira de Trens Urbanos
Administração Central
Tel. (61) 2107-8397
Tel. (21) 99192-1980

De: Paulo Cesar Barbosa de Moraes Junior <pmoraes@cbtu.gov.br>
Enviada em: terça-feira, 1 de julho de 2025 10:40
Para: Bruno de Alcantara <bruno.alcantara@cbtu.gov.br>
Cc: Mayara Suzart Gomes <mayara@cbtu.gov.br>; Reginaldo Oliveira <reginaldooliveira@cbtu.gov.br>; GETIN - Gerencia TÃ©cnica de Tecnologia da InformaÃ§Ã£o e ComunicaÃ§Ã£o <getin@cbtu.gov.br>; Gerencia Geral de LicitaÃ§Ã£o <galic@cbtu.gov.br>
Assunto: Re: Fw: SOLICITAÇÃO DE ESCLARECIMENTO - PREGÃO ELETRONICO 90005/2025 - COMPANHIA BRASILEIRA DE TRENS URBANOS

Prezados,

Considerando a solicitação do pregoeiro abaixo, segue para atendimento.

Atenciosamente,
Em 01/07/2025 09:50, Licitações Fase Externa escreveu:

> Prezados, segue pedido de encaminhamento para área demandante.
>
> Atenciosamente
> Reginaldo
>
> ---------- Mensagem encaminhada ----------
> De: "RAPHAEL OLIMPIO FERREIRA" <raphael.ferreira@algar.com.br>
> Data: 01/07/2025 09:15
> Assunto: SOLICITAÇÃO DE ESCLARECIMENTO - PREGÃO ELETONICO 90005/2025 - COMPANHIA BRASILEIRA DE TRENS URBANOS
> Para: "licitacao@cbtu.gov.br" <licitacao@cbtu.gov.br>
> Bom dia
>
> Venho por meio deste solicitar esclarecimento quanto aos pontos abaixo.
>
> Questionamento 1:
>
> Entendemos que a solução deve implementar mecanismos capazes de detectar e mitigar ataques que façam o uso não autorizado de recursos de rede, automaticamente, tanto para IPv4 e IPv6.
> Nosso entendimento está correto?
>
> Questionamento 2:
>
> Entendemos que a solução de proteção contra-ataques de negação de serviços deve ser disponibilizada no backbone da CONTRATADA, não sendo permitida a subcontratação da mesma, ou seja, para que a integridade dos dados e informações trafegadas não sejam comprometidas, não será permitido que a CONTRATADA realize o redirecionamento do tráfego para infraestruturas de terceiros para que estes realizem a mitigação dos ataques e não será aceito bloqueio de ataques de DOS e DDOS por ACLs em roteadores de bordas da contratada.
> Nosso entendimento está correto? Caso o entendimento esteja correto, as licitantes deverão comprovar que possuem infraestrutura própria de proteção contra ataques de negação de serviços?

Atenciosamente.

Raphael Olimpio Ferreira

Analista de Licitações
II
Diretoria Governo

34 99182-2859

--

Paulo Cesar B. de Moraes Junior
Gerente Geral de Licitação - GALIC
Gestor de Conformidade
Presidente da Comissão de Ética
Companhia Brasileira de Trens Urbanos - CBTU
Setor Bancário Norte - Quadra 1 - Bloco B - Ed. CNC
13º andar - Brasília - DF, 70041-902
pmoraes@cbtu.gov.br
www.cbtu.gov.br