Gmail

Nelson de Espindola Vasconcelos .. <nelson.vasconcelos@tjpb.jus.br>

QUESTIONAMENTOS - PREGÃO ELETRÔNICO – N º 023/2023

1 mensagem

'Francolino Rodrigues da Mata Júnior' via prege <prege@tjpb.jus.br> 7 de agosto de 2023 às 18:58
Responder a: Francolino Rodrigues da Mata Júnior <franco.damata@servix.com>
Para: prege@tjpb.jus.br

Sr. Pregoeiro,

e-mail: prege@tjpb.jus.br

Na intenção da nossa participação no certame PREGÃO ELETRÔNICO – N º 023/2023, solicito a gentileza em encaminhar resposta aos esclarecimentos para as questões abaixo:

QUESTIONAMENTO 01:

Em relação ao item 4.4.27 que descreve "Deverá ter a capacidade de gerar relatórios detalhados baseados em tráfego/acessos/atividades do usuário.". A geração de relatórios permite que as equipes de administração de rede e segurança possuam informações relevantes sobre o cenário do ambiente tecnológico, garantindo o gerenciamento de um grande volume de registros e permitindo a pesquisa de eventos específicos através de diversos critérios de pesquisa. A geração de relatórios também são extremamente uteis em momentos críticos, como recebimento de ataques ou falhas nos ambientes de aplicações WEB. Deste modo, entendemos que a solicitação de geração de relatórios baseadas em tráfego, acessos e atividades consiste em um detalhamento de endereço IP de origem dos acessos, porta de destino das aplicações acessadas, tempo de resposta da aplicação, ataques detectados pela funcionalidade de WAF, entre outros, de modo a permitir análises históricas e auxiliar nos processos de manutenções preventivas, de troubleshooting, de planejamento de capacidade e de análise da experiência dos usuários finais no acesso das aplicações. Está correto nosso entendimento?

QUESTIONAMENTO 02:

Através da caracteres randômicos, a proteção contra-ataques do tipo MITM dificultam ataques direcionados à aplicação. Entendemos que a solicitação do item 4.6.21 que descreve "Ter a capacidade de proteção para ataques do tipo Man-in-the-middle (MITM).", refere-se à ofuscação do nome de parâmetros sensíveis das aplicações. Está correto nosso entendimento?

QUESTIONAMENTO 03:

O item 4.6.9 descreve "A solução deverá possuir funcionalidade de proteção positiva contra ataques como acesso por força bruta.". Desta forma a proteção contra ataques de força bruta varia de acordo com as características de cada aplicação. Entendemos que a solicitação refere-se aos parâmetros de número máximo de tentativas e tempo de bloqueio. Está correto nosso entendimento?

QUESTIONAMENTO 04:

O item 4.6.47 descreve "A solução deve ser capaz de funcionar como Terminador de sessões SSL para a aceleração de tráfego." , no qual é solicitado estabelecimento de sessões entre o cliente e a solução, entendemos que para estabelecimento seguro de sessões, a solução deve estabelecer uma segurança de autenticação mútua de

certificado na comunicação com o cliente. Está correto nosso entendimento?

QUESTIONAMENTO 05:

Em ambiente de aplicações web, existem aplicações que operam utilizando HTTPS. O processo de decriptografia impacta na performance das aplicações. Entendemos que a solicitação do item 4.6.46 que descreve "Deverá ser capaz de fazer aceleração de SSL, onde os certificados digitais são instalados na solução e as requisições HTTP são enviadas aos servidores sem criptografia.". Diante da aceleração SSL, onde os certificados digitais são instalados na solução, deve ocorrer através da configuração de Perfect Forward Secrecy, OCSP (Online Certificate Status Protocol) Stapling e ALPN (Application Layer Protocol Negotiation). Está correto nosso entendimento?

Desde já agradeço a atenção.