TRIBUNAL DE JUSTIÇA
DO ESTADO DA BAHIA

DOD
DOCUMENTO DE OFICIALIZAÇÃO DA DEMANDA

1 IDENTIFICAÇÃO DA DEMANDA

1.1 Título:

Contratação de Serviço continuado de Solução de Segurança Web Application firewall (WAF)

1.2 Unidade Demandante:

Coordenação de Suporte Técnico

1.3 Responsável pela Unidade Demandante:

Nome: Leonardo Gomes Dias
Matrícula: 969.240-1
Telefone: (71) 3372-1505
E-mail: lgdias@tjba.jus.br

1.4 Indicação do Gestor do contrato:

Nome: Leonardo Gomes Dias
Matrícula: 969.240-1
Telefone: (71) 3372-1505
E-mail: lgdias@tjba.jus.br

1.5 Indicação do Fiscal Titular do contrato:

Nome: Cleiton Rodrigues de Carvalho
Matrícula: 968.544-8
Telefone: (71) 3372-1544
E-mail: clrocarvalho@tjba.jus.br

1.6 Indicação do Fiscal Suplente do contrato:

Nome: Thales Bruno Lima Malheiro
Matrícula: 968324-0
Telefone: (71) 3372- 7581
E-mail: tblmalheiro@tjba.jus.br

2 CONTEXTO DE NEGÓCIO

2.1 Situação Atual:

O Tribunal de Justiça da Bahia possui atualmente diversos sistemas web, tanto para uso interno de servidores e colaboradores como o Gefre, Rhnet, Siga como sistemas utilizados interna e externamente como PJE, Projudi, e-Saj, entre outros.

Esses sistemas são protegidos por uma série de mecanismos que fazem parte da infraestrutura do TJBA, porém com a evolução constante dos métodos de ataques que tem como finalidade a extração, modificação e até a indisponibilidade dos dados faz-se necessário a utilização de ferramentas específicas para a proteção dos dados expostos na internet.

Diante destes fatos algumas questões se tornaram latentes: como proteger informações que trafegam fora do perímetro de segurança da rede? Como garantir o tráfego seguro de informações? Como melhorar a disponibilidade de serviços oferecidos?

No passado, a principal solução de tecnologia para segurança de aplicações web era de responsabilidade do firewall. A tecnologia evoluiu e foi criado o Web Application Firewall para analisar e proteger de ameaças que estão além da capacidade dos firewalls tradicionais, criando uma barreira entre serviço baseado na web e as principais ameaças.

O WAF impede a exposição de dados não autorizada em um site ou aplicativo baseado na web, filtrando e bloqueando automaticamente o tráfego de dados potencialmente maliciosos, além de permitir a definição de regras para evitar os ataques mais comuns.

2.2 Descrição da Oportunidade ou do Problema:

a) Diante das considerações acima efetuadas, fica claro que para uma organização com diversos sistemas disponibilizados através da web, é essencial possuir um mecanismo que lhe dê uma nova camada de proteção, que tenha a capacidade de tomar ações rápidas para conter ameaças com rapidez e eficiência e proporcionar alto desempenho para aplicações web.

Além das características acima, espera-se que a tecnologia WAF, seja capaz de rapidamente superar uma ampla variedade de questões relacionadas à segurança, identificar e bloquear ataques utilizando base de dados de assinaturas e reputação de IP, automaticamente aprender a estrutura das aplicações Web e o comportamento dos usuários e implementar proteção de forma automatizada para estas aplicações; proteção contra indisponibilidades provenientes de acesso em massa (DDOS), deve conter as assinaturas de robôs conhecidos e resetar conexões provenientes destes robôs, balanceamento de sessões com implementação de persistência, implementar persistência baseada em cookies e em JSP Session ID, reconhecer e remediar ataques de dia zero, prover o mínimo impacto no ambiente do TJBA; estatísticas e visibilidade de acesso as páginas publicadas na Web, além de proteger os sistemas web das principais ameaças contidas no OWASP Top 10 mais atual. (https://owasp.org/www-project-top-ten/).

Também se espera que o Web Application Firewall seja capaz de ser implementado no modo Proxy ou modo transparente, suportar redirecionamento e reescrita de requisições e respostas HTTP, roteamento de tráfego por política, ser capaz de armazenar certificados digitais de Autoridades Certificadoras, gerar CSR para ser assinado por uma CA.

Feitas todas as considerações, a área técnica sugere e solicita a contratação de serviço continuado de uma solução de segurança Web Application firewall (WAF) com suporte e garantia de 36 meses.

Indica-se abaixo os requisitos mínimos da solução:

A solução deve ser em appliance e com alta disponibilidade, permitindo tanto monitorar como gerar logs dos sistemas gerenciados. Deve possuir interfaces de 1Gbps RJ-45, interfaces de 1Gbps SFP e interfaces de 10Gbps SFP+.

Capacidade para ações de controle:

Notificar, Restringir, Impor Políticas, mitigar ataques.

Por se tratar de um ambiente crítico e de alta complexidade, a nova contratação deve cobrir também todos os custos necessários para implementação das novas soluções com apoio presencial e operação assistida.

2.3 Motivação da Demanda:

a) Contratação de Serviço continuado contemplando o hardware e software da solução para proteção de aplicações web, detecção e prevenção contra ameaças;

b) Suporte técnico avançado 24X7;

c) Redução de recursos gerais administrativos necessários para a gestão de segurança da rede;

2.4 Resultados Pretendidos:

a) Garantir à disponibilidade da solução que fornece proteção contra ataques virtuais;

b) Alta disponibilidade e integridade do ambiente tecnológico deste Tribunal.

c) Manter as aplicações web mais seguras, com a implementação de regras personalizadas, minimizando os problemas relacionados, cite-se:

- Injeção de dados;
- Exposição de dados confidenciais;
- Quebra de sessão e gerenciamento de sessões;

d) Maturidade do processo de monitoramento, através da predefinição e personalização de gráficos de monitoramento e envio de notificações.

2.5 Alinhamento Estratégico:

a) Garantir a disponibilidade de sistemas essenciais de TIC;

b) Garantir a infraestrutura e o ambiente seguro as atividades finalísticas;

c) Aquisição prevista no Plano de Contratações 2020 como: Serviços de suporte e ampliação da infraestrutura de proteção de dados.

d) Alinhamento com os objetivos estratégicos da Resolução 211/2015 do CNJ: Objetivo 8: Aprimorar a segurança da informação;

3 CONTEXTO DA DEMANDA

3.1 Ciclo de Vida da Demanda.

3.1.1 Qual a expectativa de tempo de utilização ou validade da solução objeto da demanda?

[ ] Menos de 1 ano [x] De 1 a 3 anos [ ] Mais de 3 anos

3.1.2 Trata-se de uma demanda com caráter definitivo ou temporário? Há algum fato já conhecido que poderá implicar a descontinuidade da demanda ou a sua substituição?

Trata-se a demanda da contratação de Appliance (embora possa ser ofertado em apenas software), levando em consideração a defasagem tecnológica comum no mercado de tecnologia numa média de tempo de 5 anos, caracteriza-se a aquisição dos equipamentos de caráter temporário. Contudo, é também comum no mercado que os fabricantes de tecnologia forneçam os serviços continuados de garantia e suporte por até 5 anos após o encerramento da comercialização de determinada tecnologia, permitindo assim que estes tenham sua vida útil prolongada e, em caso de falhas irrecuperáveis, procedam a imediata correção ou substituição dos aparatos tecnológicos contratados.

3.2 Clientes que farão uso da solução (objeto da demanda) ou serão beneficiados.

3.2.1 Demanda de âmbito Interno ao TJBA:

Selecione uma das opções seguintes:

[ ] Até 1 Unidade [ ] 2 ou 3 Unidades [x] 4 ou mais Unidades do TJBA

Caso a sua demanda tenha impacto em mais de uma unidade, justifique a opção selecionada:

Solução de Segurança para aplicações WEB do Tribunal de Justiça que é utilizada pela maioria das Unidades. São exemplos destas aplicações, por exemplo, PJE, PROJUDI, SIGA, RHNET.

3.2.2 Demanda de âmbito Externo ao TJBA:

Selecione uma das opções seguintes:

[ ] Até 1 Órgão [ ] 2 ou 3 Órgãos [x] 4 ou mais Órgãos

Caso a sua demanda tenha impacto em mais de um Órgão, justifique a opção selecionada:

Solução de Segurança para aplicações WEB do Tribunal de Justiça utilizada por Advogados, MP, PGE. São exemplos destas aplicações, principalmente, PJE e PROJUDI.

3.3 Expectativa de entrega da solução.

Em até quanto tempo ou em até que data a solução demandada deve ser implantada para não perder sua utilidade ou a oportunidade que se apresenta?

O Appliance deve ser entregue no prazo de 45 (quarenta e cinco) dias, contatos da data de assinatura do contrato.

A expectativa de instalação da solução é de 30 dias úteis após o recebimento, deve-se considerar por outro lado, um período adicional para implementação de controles extraindo o máximo de usabilidade da solução.

A contratação do serviço de garantia e suporte de que trata o presente processo deve ser realizado pelo período de 36 meses, contados a partir do aceite de técnico emitido pela área técnica, de forma a garantir cobertura para assistência e suporte técnico para o ambiente descrito neste documento.

3.4 Integrante Demandante Titular:

Informe os dados do servidor:

Nome: Cleiton Rodrigues de Carvalho

Matrícula: 968.544-8

Telefone: (71) 3372-1544

E-mail: clrocarvalho@tjba.jus.br

3.5 Integrante Demandante Suplente:

Informe os dados do servidor que responderá nas ausências ou impedimentos do Integrante Demandante Titular.
A fim de dar celeridade ao processo, é necessário que o suplente acompanhe toda a evolução da contratação conjuntamente com o titular.

Nome: Thales Bruno Lima Malheiro

Matrícula: 968324-0

Telefone: (71) 3372- 7581

E-mail: tblmalheiro@tjba.jus.br

4 REFERÊNCIAS

Não se aplica

5 AUTORIZAÇÃO

De acordo, encaminhe-se à SETIM.

Em: 15/07/2020.

_____

Titular da Unidade Demandante