## Pregão/Concorrência Eletrônica

- **Visualização de Recursos, Contrarrazões e Decisões**

**RECURSO :**

A(AO) ILUSTRÍSSIMO(A) SENHOR(A) PREGOEIRO(A) DA COMISSÃO PERMANENTE DE LICITAÇÃO DA PRODAM – PROCESSAMENTO DE DADOS AMAZONAS S.A.

Ref.: PREGÃO ELETRÔNICO SRP Nº 14/2022

WAVEZ TECNOLOGIA E COMUNICAÇÃO DIGITAL LTDA, pessoa jurídica de direito privado, inscrita no CNPJ sob o nº 12.910.896/0001-25, com sede na SHIS QI 21, Bloco C, Sala 307, Lago Sul – Brasília/DF, CEP: 71655-200, representante legal Max Maurício Meira, inscrito sob CPF nº 398.264.141-15, vem tempestivamente, à presença de Vossa Senhoria, por meio de seu representante legal, pautada nas legislações pertinentes, bem como o inciso XVIII do art. 4 da Lei no 10.520/02, apresentar

RAZÕES DE RECURSO ADMINISTRATIVO

em face da decisão administrativa que desclassificou a empresa Wavez Tecnologia em Prova de Conceito conforme o item 17.2.8, pelas razões de fato e de direito a seguir aduzidas.

Trata-se de licitação na modalidade PREGÃO ELETRÔNICO, tipo MENOR PREÇO DO ITEM, no modo de disputa ABERTO e FECHADO cujo objeto é "Contratação de solução de cibersegurança, auditoria e prevenção de ameaças à base de dados não estruturados em endpoint, na modalidade de subscrição, incluindo garantia, serviço de instalação e treinamento, visando ampliar a capacidade de atendimento ao ambiente de desktops e servidores da Prodam e seus clientes em relação ao combate às ameaças cibernéticas, conforme especificações detalhadas no Termo de Referência", conforme condições, quantidades e exigências estabelecidas no Edital e seus anexos.

1. DO CABIMENTO E DA TEMPESTIVIDADE

Inicialmente, salienta-se que nos termos do item 4.3.1 do Edital do presente certame, "O proponente que desejar recorrer contra decisões do Pregoeiro poderá fazê-lo, manifestando a intenção de recurso com registro da síntese de suas razões no espaço previsto no próprio sistema eletrônico, sendo necessário juntar memoriais no prazo de 03 (três) dias uteis".

É sabido que as compras e alienações publicas devem ser precedidas obrigatoriamente de processo de licitação, excetuadas as hipóteses de dispensa e inexigibilidade previstas na Lei Geral de Licitações (Lei Federal no 8.666/93).

Em que pese o alto poder regulamentar conferido ao instrumento convocatório de uma licitação, a Administração licitante encontra-se vinculada ao atendimento dos limites e imposições legais que tornem o processo válido e eficaz para conferir a devida legalidade ao ato da contratação, assegurando com isso o contraditório aos licitantes.

A Lei Geral de Contratos e Licitações (Lei 8.666/93) já fazia prever, em seu artigo 109, a possibilidade de recurso pelas licitantes interessadas quando o legislador incluiu na edição da Lei do Pregão (Lei 10.520/02):

Art. 4o A fase externa do pregão será iniciada com a convocação dos interessados e observará as seguintes regras:
XVIII - declarado o vencedor, qualquer licitante poderá manifes-tar imediata e motivadamente a intenção de recorrer, quando lhe será concedido o prazo de 3 (três) dias para apresentação das razões do recurso, ficando os demais licitantes desde logo intimados para apresentar contrarrazões em igual número de dias, que começarão a correr do término do prazo do recorren-te, sendo-lhes assegurada vista imediata dos autos; (Grifamos)
Nos mesmos moldes, é o estabelecido pelo edital:
12.1. Após a habilitação e aprovação da solução ofertada na PROVA DE CONCEITO (POC), conforme itens 10 e 11 deste edi-tal, a licitante vencedora será declarada como "Habilitada" no sistema Compra Aberta e será aberto o prazo para intenção de recurso, momento no qual qualquer das licitantes poderão em até 24 (vinte e quatro) horas, através do sistema Compra Aber-ta, manifestar motivadamente em campo próprio a intenção de recorrer, argumentando sucintamente os motivos, para a apre-ciação do(a) Pregoeiro(a).
12.2. O(A) Pregoeiro(a) negará admissibilidade ao recurso quan-do:
a) interposto sem motivação ou não estiver devidamente fun-damentado; b) apresentado fora do prazo estabelecido (intem-pestivamente); ou c) não corresponder ao objeto deste certame.
12.2.1. A falta de manifestação no prazo previsto no item 12.1 e motivação da intenção de recorrer das licitantes importará de-cadência do direito de recurso.
12.2.2. Admitido o recurso será concedido o prazo de 3 (três) dias uteis para apresentação de suas razões pela(s) licitante(s) recorrente(s), sendo que a admissão da intenção não é comuni-cada pelo sistema Compra Aberta de forma automática, deven-do a(s) licitante(s) que apresentar(am) a intenção acompa-nhar(em) a realização do juízo de admissibilidade diretamente no portal Compra Aberta.
(...)
Sendo realizada a intenção de recorrer da decisão em 07/02/2023, resta plenamente admissível os presentes memoriais recursais. Nestes termos, é tempestivo o presente recurso.

2. DA PRELIMINAR DE IMPOSSIBILIDADE DE AMPLA DEFESA E CONTRADITÓRIO

Insta consignar que, de maneira preliminar, conforme será demonstrado nas razões recursais, a presente peça defensiva não é municiada de todo o conteúdo que ensejou a desclassificação da ora recorrente.

Em resultado de Prova de Conceito dever-se-ia constar, de maneira individualizada, por meio da comissão da POC, todos os itens e motivações de possíveis inconformidades que ensejariam em desclassificação do concorrente, no pregão eletrônico.

A despeito do alegado, e de maneira respeitosa no que tange a decisão da autoridade do pregão, não foi isto que ocorreu no presente certame. O douto pregoeiro somente elencou os pontos entendidos como desatendimento à tabela de anexo 1-A, não informando as motivações de inconformidade.

Adentrando em questões técnicas da Tecnologia da Informação – TI, é possível entender que cada suposto erro/desatendimento geraria um informação denominada LOG, sendo possível com este LOG a possibilidade de correção da inconformidade do sistema, da informação, do terminal ou do arquivo executável ou da funcionalidade.

Ora, a não disponibilização deste LOG impediu a imediata correção do suposto erro, como a próxima cognição do erro e motivação para as razões recursais do presente Recurso Administrativo.

Em outras palavras, não se sabe, minimamente, quais foram os motivos da suposta inconformidade de informações entre a funcionalidade e o ambiente disponibilizado para a realização do teste.

A não disponibilização do LOG em decisão fundamentada do pregoeiro pela desclassificação, impede o exercício da ampla defesa recursal em face da não fundamentação de decisão terminativa de mérito.

De igual forma, a supracitada não fundamentação em decisão de desclassificação não revela se a responsabilidade pelos supostos apontados erros seria da funcionalidade testada ou do próprio ambiente recebedor do teste, ensejando a real e premente dúvida quanto à disfuncionalidade do programa ou a inaptidão do ambiente disponibilizado, fato que sem dúvida alguma afastaria a possibilidade de êxito de qualquer outro competidos concorrente.

Dadas essas premissas básicas, mesmo sem a disponibilização dos LOGS dos erros/inconformidades, nas presentes razões recursais o recorrente demonstrará, em máximo esforço, os motivos relativos a possíveis inconformidade e elencando que as possíveis falhas decorrem de culpa exclusiva do ambiente e das máquinas disponibilizadas pela PRODAM, fato que inegavelmente enseja a necessidade da retomada da Prova de Conceito após sanadas as inconformidades e os vícios de ambiente, conforme pedido principal.

Outro ponto que sustenta o alegado acima, diz respeito ao fato de que o mesmo sistema ora testado já roda em pequenas funcionalidades e perfeição em ambientes com as mesmas características do outrora testado na POC, fato que enseja a tomada de diligencias por parte do pregoeiro, com fito de atestar que não se tratava de falha da funcionalidade e sim de inconformidade do ambiente.

## 3. DAS RAZÕES PARA APRESENTAÇÃO DO RECURSO

Este recurso é interposto em decorrência de decisão prolatada no dia 07/02/2023, pela qual o Sr. Pregoeiro entendeu por desclassificar a Recorrente informando o não preenchimento dos requisitos:

"Encerrada a prova de conceito realizada com a empresa Wavez Tecnologia no dia 03/02/2022. Informamos que em desatendimento aos itens: 13.2.1.2.1; 13.2.1.2.4; 13.2.1.2.4; 13.2.4.2; 13.2.5.2; 13.2.7.12; 13.2.7.13; 13.2.7.14; 13.2.7.15; 13.2.8.3; 13.2.8.5; 13.2.8.6; 13.2.8.9; 13.2.8.15; 13.2.9.1. 13.2.9.1.1;13.2.9.1.2; 13.2.9.1.4. 13.2.9.1.5; 13.2.9.1.6; 13.2.9.1.7; 13.2.9.1.8; 13.2.10.1; 13.2.10.1.1; 13.2.10.1.2, 13.2.10.1.3, 13.2.10.1.4, 13.2.10.1.5, 13.2.11.1; 13.2.11.11 13.2.11.12, 13.2.11.1.3, 13.2.1114 13.2.11.1.5, 1321116 1321117 3.2.11.1. 13.2.11.1.10; 13.3.6.10; 13.3.11.15. 13.3.11.16; 13.3.11.20 dos requisitos e funcionalidades da solução tecnológica do Anexo 1-A - Tabela de Demonstração de Atendimento. A empresa Wavez Tecnologia está desclassificada conforme item 17.2.8 do termo de referência parte integrante do edital."

Todos os itens arrolados pelo pregoeiro são relativos à tabela de Demonstração de Atendimento, ou seja, atinentes a especificações e comprovações de itens técnicos da solução.

Ocorre que, conforme será demonstrado nas razões do presente recurso as inconformidades e supostos desatendimentos devem ser atribuídas a diversas falhas no ambiente de Prova, gerando insuficiências de comunicação entre os sistemas, bem como considerando que itens tratados como descumpridos foram devidamente demonstrados.

## 4. DOS REQUISITOS E FUNCIONALIDADES DA SOLUÇÃO TECNOLÓGICA

Compulsando a decisão do pregoeiro, faz-se necessário elencar todos os pontos trazidos como fundamentadores da desclassificação, descrevendo todas as inconformidades e justificativas técnicas, item a item:

Antes de adentrar ponto a ponto nos itens que supostamente a desclassificação da ora recorrente, resta necessário fixar premissas básicas que servirão como justificativa para diversos itens, não nos furtando em apresentar defesa desses mesmos itens, de maneira específica:

• Problemas na instalação inicial dos agentes, por configuração errônea dos atributos de rede do cliente, impossibilitando a comunicação e distribuição adequada em relação ao quantitativo de máquinas para demonstração dos itens do edital. Fora fornecido somente escopo extremamente reduzido (6 máquinas);
• Foi solicitada a instalação do agente com o usuário da máquina utilizando o privilégio de administrador local, para que se possa liberar a comunicação do agente com a central. Esta configuração essencial permite que o firewall

local do Windows abra portas de comunicações entre o endpoint e a console de gerenciamento;
• Para demonstração dos itens, seria necessário a instalação de processos maliciosos em um ambiente seguro. Por segurança e otimização, itens foram demonstrados por comprovação de uso da api do VirusTotal – solução embarcada com dezenas de motores de análise de vulnerabilidade, portanto, entende-se que todos os itens relativos a ameaças maliciosas/vírus encontram-se plenamente demonstrados, não havendo motivo para a de classificação quanto a estes itens.

Componentes do Windows nas máquinas utilizadas para a demonstração, de propriedade da Prodam

13.2.1.2.1 – Agentes para endpoints - Compatibilidade - Windows 7 32bits e 64 bits;

Resposta:
• Problema relacionado a componentes do WINDOWS instalado no en-dpoint testado, não permitindo o pleno funcionamento do agente da solução ofertada no sistema operacional Windows.
• Vale ressaltar que foi disponibilizado apenas um computador com Windows 7 32bits, que apresentou diversos problemas já na instalação do agente, impossibilitando a execução do teste.

13.2.1.2.4 – Agentes para endpoints – Compatibilidade - Windows Server em suas versões 2012 R2, 2016 e 2019, 32 bits e 64 bits.

Resposta:
• Alguns versionamentos do Sistema Operacional de endpoint não fo-ram disponibilizados pela PRODAM, não sendo afirmar a desclassifi-cação quanto a este ponto, tendo em vista que o próprio órgão nem mesmo oportunizou o teste, em face da inexistência da versão. Ade-mais, o endpoint disponibilizado para teste apresentou falha de componentes internos, impossibilitando o teste. Desta forma, há que se considerar falha no sistema operacional pois a mesma versão tes-tada está plenamente operacional em dezenas de clientes, incluindo bancos.

13.2.4.2 – Agentes para endpoints – Segurança - Deve possuir proteção contra desinstalação ou interrupção do agente.

Resposta:
• Item demonstrado. Embora o agente tenha sido removido no diretó-rio "adicionar e remover programas", os processos continuavam em execução. Tal fato foi atestado e comprovado pelo avaliador, no mo-mento da POC. Quanto a este item, entendemos pelo seu fiel cum-primento, não ensejando a desclassificação da empresa.

13.2.5.2 – Agentes para endpoints – Inteligência Artificial - Capacidade de aprendizado de comportamento de usuários para aprimoramento das detecções de comportamentos suspeitos.

Resposta:
• Todo sistema composto por motores de inteligência artificial depende de motores secundários, chamados MACHINE LEARNING ou "apren-dizado de máquina". Para ocorrer o aprendizado, são necessários principalmente dois itens, a saber: 1) tráfego de dados, ou seja, a máquina tem que estar sendo plenamente utilizada e, 2) Tempo de aprendizado, ou seja, para haver o aprendizado de determinado comportamento, deve haver repetições diversas com as mesmas ca-racterísticas, populando desta forma, o banco de dados. No teste efe-tuado, instalou-se o agente e, SEM ATIVIDADE NA MÁQUINA e SEM TEMPO HÁBIL para a geração de conteúdo de aprendizado. Desta forma, procurou-se evidência do funcionamento, o que é tecnicamen-te impossível diante das condições descritas. Quanto a este item, en-tendemos a plena satisfação da demonstração da respectiva funcio-nalidade na POC, havendo capacidade de aprendizado, mesmo que o resultado necessite de prazo na absorção do sistema.

13.2.7.12 – Agentes para endpoints – Outras Funcionalidades - Identificação de tráfegos de entrada e saída, com base em endereços MAC, frame types, protocolos, endereçamento IP e portas (serviços).

Resposta:
• A identificação dos tráfegos de entrada e saída, com base em endereçamento de adaptador de rede (mac) só é possível mediante a abertura de portas no sistema de segurança do cliente (firewall e similares). Não conseguimos qualquer evidência que comprovasse que as portas necessárias estivessem abertas. Pelos sintomas de falta de alimentação de dados no servidor, as portas não estavam abertas conforme solicitado.

13.2.7.13 - Agentes para endpoints – Outras Funcionalidades - Capacidade parametrizada de coletar, registrar e armazenar todas as conexões (TCP) ou transmissões (UDP) de rede, incluindo informações sobre endereços IP, portas de origem e destino e domínios DNS.

Resposta:
• As portas necessárias para permitir o tráfego de rede adequado entre o endpoint e o servidor da aplicação possivelmente não estavam abertas, evidenciado pela falta de alimentação do servidor com os dados dos endpoints, além de não ter havido tempo hábil de aprendizado de tráfego.
Outro ponto a ser considerado é o fato do número de máquinas disponibilizados ter sido de apenas 6, reduzindo drasticamente o volume de dados trafegados, onerando em maior tempo de coleta de dados para normalização em servidor.

13.2.7.14 - Agentes para endpoints – Outras Funcionalidades - Informar programas e processos em execução em tempo real.

Resposta:
• Para haver a alimentação, em tempo real das informações dos endpoints, são necessárias diversas ações, por parte do cliente, como a abertura de portas de comunicação, bem como a utilização massiva dos equipamentos monitorados. O que experienciamos foi a disponibilização de apenas 6 máquinas, sendo que algumas delas com problemas de sistema operacional, problemas em componentes que impossibilitaram a instalação do agente, reduzindo drasticamente o volume de dados de amostragem, além de portas de comunicação bloqueadas, o que tornou impossível a execução dos testes. Ademais, conforme demonstrado, o fato de só haver um servidor da PRODAM operando máquina, e este único servidor ausentar-se no meio da POC, impediu o pleno ateste do item em comento, pela falta de conteúdo/processos em execução em tempo real.

13.2.7.15 - Agentes para endpoints – Outras Funcionalidades - Registro de softwares (instalados, executados e em execução), com possibilidade de mitigação de softwares vulneráveis em execução bem como a data de instalação de cada item.

Resposta:
• Para haver registro de softwares instalados, algumas premissas devem ser consideradas. 1) Plena comunicação dos agentes instalados nos endpoints com o servidor, o que não ocorreu devido a bloqueio de portas. 2) Tempo de aprendizado (machine learning), o que também não ocorreu por não haver tempo suficiente, considerando que a POC foi encerrada pelo pregoeiro em 3h20m, sendo que o edital contemplava 4 horas apenas para INSTALAÇÃO da ferramenta e não estipulava limite de tempo para a execução dos testes. Desta forma, não há tempo hábil de aprendizado de máquina e sem tráfego suficiente, pelos problemas já citados anteriormente. Resta clara a impossibilidade causada pelo próprio ambiente disponibilizado, considerando, inclusive, que atualmente o sistema é utilizada por clientes com mais de 20 mil máquinas instaladas.

13.2.8.3 – Agentes para endpoints – Monitoramento - Monitoramento de páginas web acessadas e upload e download de arquivos a partir de páginas web.

Resposta:
• Para haver monitoramento de páginas web, deve-se considerar que o básico deve ser suprido pelo cliente, possibilitando a demonstração, a saber: Portas de comunicação desbloqueadas, tempo mínimo de aprendizado de máquina (para esta solução), computadores em plenas condições de receber o agente e atividade de trabalho nos equipamentos. Nenhuma das condições acima foi observada pelo analista responsável pela POC.

13.2.8.5 - Agentes para endpoints – Monitoramento - Tentativas de evitar a coleta de dados da solução;

Resposta:
• A coleta de dados da solução precisaria ser efetiva para que houvesse uma tentativa de bloqueio. Porém, devido à falta de permissão interna de tráfego de rede na infraestrutura do cliente, foi impossível sequer evidenciar o tráfego de dados (coleta de dados), o que inevitavelmente impediu o teste de tentativa de bloqueio.

13.2.8.6 - Agentes para endpoints – Monitoramento - Tentativas de desinstalar a solução;

Resposta:
• Apesar do sistema estar disponível para desinstalação, os processos continuaram ativos, evidenciando que o sistema não teria sido paralisado com a tentativa. Desta forma, FOI DEMONSTRADO o cumprimento deste item.

13.2.8.9 - Agentes para endpoints – Monitoramento - Monitoramento de operações (acesso, cópia, modificação, duplicação e exclusão) com arquivos no disco local, dispositivos USB, dispositivos móveis conectados, drives CD/DVD, mídias removíveis, compartilhamento em rede ou em nuvem e acesso a drivers de rede, com a respectiva coleta de evidências.

Resposta:
• Para haver demonstração da manipulação de arquivos, primeiramente é necessário que todas as portas de comunicação necessárias estejam desbloqueadas. É necessário também que haja a manipulação de dados nas estações de trabalho. Como não houve comunicação entre a estação de trabalho e o servidor instalado, mesmo que houvesse manipulação de dados nas poucas máquinas disponibilizadas (6 ao todo, sendo duas com problemas), não seria possível realizar a análise.

13.2.8.15 - Agentes para endpoints – Monitoramento - Monitoramento e detecção de processos, drivers e serviços:

Resposta:
• Sem a plena comunicação (sem bloqueios) entre as estações de trabalho e o servidor, sem que os equipamentos estejam plenamente operacionais, e sem tempo hábil de coleta e aprendizado o item não poderia ter sido demonstrado por culpa plena e exclusiva do ambiente recebedor do teste.

13.2.9.1 - Agentes para endpoints - Proteção contra vazamento de dados - O agente deve monitorar dados classificados contra vazamento nos seguintes vetores:

Resposta:
• O vazamento de dados é caracterizado PRINCIPALMENTE por análise comportamental, o que requer invariavelmente, tempo de aprendizado de máquina associado ao motor de inteligência artificial. Salientamos que não houve o mínimo necessário, disponibilizado pelo cliente, como portas de comunicação desbloqueadas, equipamentos plenamente operacionais e tempo hábil de coleta de dados, considerando que toda a prova de

conceito foi encerrada pelo pregoeiro, em tempo consideravelmente menor do que o especificado, em edital, apenas para a instalação da solução.

13.2.9.1.1 - Agentes para endpoints - Proteção contra vazamento de dados - O agente deve monitorar dados classificados contra vazamento nos se-guintes vetores: - Print de tela, independente de ferramenta;

Resposta:
• Para haver a demonstração dos prints de tela evidenciados, a coleta de dados da estação de trabalho, pelo servidor é fator fundamental, o que foi impossibilitado pelo bloqueio das portas de comunicação e pelo tempo escasso da prova (aquém do especificado em edital), além da inexistência de massa de teste com diversos servidores operando as máquinas.

13.2.9.1.2 - Agentes para endpoints - Proteção contra vazamento de dados - O agente deve monitorar dados classificados contra vazamento nos se-guintes vetores: - Aplicações em Nuvem;

Resposta:
• Não foi disponibilizado ambiente de teste em nuvem, o que impossibi-litaria a comprovação de atendimento ou desatendimento do item.

13.2.9.1.4 - Agentes para endpoints - Proteção contra vazamento de dados - O agente deve monitorar dados classificados contra vazamento nos seguintes vetores: - Compartilhamento de Rede;

Resposta:
• O vazamento de dados é caracterizado PRINCIPALMENTE por análise comportamental, o que requer invariavelmente, tempo de aprendizado de máquina associado ao motor de inteligência artificial. Como não havia comunicação fluida entre os pontos de análise, se fez impossível a análise de um compartilhamento de rede. Salientamos que não houve o mínimo necessário, disponibilizado pelo cliente, como portas de comunicação desbloqueadas, equipamentos plenamente operacionais e tempo hábil de coleta de dados, considerando que toda a prova de conceito foi encerrada pelo pregoeiro, em tempo consideravelmente menor do que o especificado, em edital, apenas para a instalação da solução.

13.2.9.1.5 - Agentes para endpoints - Proteção contra vazamento de dados - O agente deve monitorar dados classificados contra vazamento nos seguintes vetores: - Comportamento de usuário;

Resposta:
• O vazamento de dados é caracterizado PRINCIPALMENTE por análise comportamental, o que requer invariavelmente, tempo de aprendiza-do de máquina associado ao motor de inteligência artificial. Salien-tamos que não houve o mínimo necessário, disponibilizado pelo cli-ente, como portas de comunicação desbloqueadas, equipamentos plenamente operacionais e tempo hábil de coleta de dados, conside-rando que toda a prova de conceito foi encerrada pelo pregoeiro, em tempo consideravelmente menor do que o especificado, em edital, apenas para a instalação da solução.

13.2.9.1.6 - Agentes para endpoints - Proteção contra vazamento de dados - O agente deve monitorar dados classificados contra vazamento nos seguintes vetores: - Monitorar uso de dados por P2P;

Resposta:
• O cliente não disponibilizou ambiente de teste por p2p, o que impos-sibilitaria a comprovação de atendimento ou desatendimento do item.

13.2.9.1.7 - Agentes para endpoints - Proteção contra vazamento de dados - O agente deve monitorar dados classificados contra vazamento nos seguintes vetores: - Monitoramento de arquivos acessados na rede;

Resposta:
• O acesso à rede depende de uma premissa básica, a saber: TRÁFEGO DE REDE DESBLOQUEADO, o que não foi observado em todo o desenvolvimento da prova de conceito, impossibilitando praticamente todos os testes.

13.2.9.1.8 - Agentes para endpoints - Proteção contra vazamento de dados - O agente deve monitorar dados classificados contra vazamento nos seguintes vetores: - Rastreamento do uso de mídias removíveis.

Resposta:
• Para haver coleta de informações de dados dos dispositivos plugados nas portas USB, o agente deve estar com comunicação plena com o servidor, sem bloqueios de portas ou protocolos, o que não foi observado. Não foi dado tempo para troubleshooting (análise e resolução de problemas) e a prova de conceito foi encerrada ANTES do tempo mínimo dado apenas para a instalação da solução.

13.2.10.1 – Agentes para endpoints - Detecção de vulnerabilidades - Detectar, no mínimo, as seguintes técnicas de exploração de vulnerabilidade:

Resposta:
• Para demonstração dos itens, seria necessário a instalação de pro-cessos maliciosos em um ambiente seguro E ISOLADO. Por seguran-ça e otimização, itens foram demonstrados por comprovação de uso da api do VirusTotal – solução embarcada com dezenas de motores de análise de vulnerabilidade.
• Técnicas de exploração de vulnerabilidades são executadas em ambientes ISOLADOS E CONTROLADOS, bem como OPERACIONAIS. Além disso, a coleta de dados deve ser realizada sem bloqueios de portas e protocolos, o que não foi observado.

13.2.10.1.1 - Agentes para endpoints - Detecção de vulnerabilidades - Detectar, no mínimo, as seguintes técnicas de exploração de vulnerabilidade: - Heap spray;

Resposta:
• Técnicas de exploração de vulnerabilidades são executadas em ambientes ISOLADOS E CONTROLADOS, bem como OPERACIONAIS. Além disso, a coleta de dados deve ser realizada sem bloqueios de portas e protocolos, o que não foi observado.

13.2.10.1.2 - Agentes para endpoints - Detecção de vulnerabilidades - Detectar, no mínimo, as seguintes técnicas de exploração de vulnerabilidade: - Rootkit;

Resposta:
• Técnicas de exploração de vulnerabilidades são executadas em ambientes ISOLADOS E CONTROLADOS, bem como OPERACIONAIS. Além disso, a coleta de dados deve ser realizada sem bloqueios de portas e protocolos, o que não foi observado.

13.2.10.1.3 - Agentes para endpoints - Detecção de vulnerabilidades - Detectar, no mínimo, as seguintes técnicas de exploração de vulnerabilidade: - Falha em aplicação causada pelo exploit;

Resposta:
• O cliente não disponibilizou uma aplicação que tenha sido explorada por software malicioso (exploit). Devido à falta da aplicação e, visando otimizar o tempo já escasso, o item foi demonstrado por comprovação de uso da api do VirusTotal – solução embarcada com dezenas de motores de análise de vulnerabilidade.

13.2.10.1.4 - Agentes para endpoints - Detecção de vulnerabilidades - Detectar, no mínimo, as seguintes técnicas de exploração de vulnerabilidade: - Ataque Rop;
Resposta:
• Técnicas de exploração de vulnerabilidades são executadas em ambientes ISOLADOS E CONTROLADOS, bem como OPERACIONAIS. Além disso, a coleta de dados deve ser realizada sem bloqueios de portas e protocolos, o que não foi observado.

13.2.10.1.5 - Agentes para endpoints - Detecção de vulnerabilidades - Detectar, no mínimo, as seguintes técnicas de exploração de vulnerabilidade: - Ataque SEHOP;

Resposta:
• ISOLADOS E CONTROLADOS, bem como OPERACIONAIS. Além disso, a coleta de dados deve ser realizada sem bloqueios de portas e protocolos, o que não foi observado.

13.2.11.1 – Agentes para endpoints - Coletas para investigação - Permitir a coleta de, no mínimo, as seguintes informações para investigação, sendo remoto ou não:

Resposta:
• A coleta dos dados foi totalmente prejudicada pela falta de comunicação entre os pontos monitorados e o servidor, uma vez que as portas e/ou protocolos necessários estavam bloqueados no ambiente do cliente, agravado pelo fato de não ter sido disponibilizado tempo para a investigação e resolução do problema, uma vez que a prova de conceito foi encerrada totalmente, antes do tempo previsto apenas para instalação da solução e sem a apresentação de LOG dos erros.

13.2.11.1.1 - Agentes para endpoints - Coletas para investigação - Permitir a coleta de, no mínimo, as seguintes informações para investigação, sendo remoto ou não: - Arquivos escritos;

Resposta:
• Novos arquivos detectados nas estações de trabalho são captados pelo agente, o qual precisa enviar os dados para o servidor central, que faz o correlacionamento e alertas. Salientamos que a coleta dos dados foi totalmente prejudicada pela falta de comunicação entre os pontos monitorados e o servidor, uma vez que as portas e/ou protocolos necessários estavam bloqueados no ambiente do cliente, agravado pelo fato de não ter sido disponibilizado tempo para a investigação e resolução do problema, uma vez que a prova de conceito foi encerrada totalmente, antes do tempo previsto apenas para instalação da solução, evitando assim qualquer tipo de defesa por parte da LOQED SYSTEMS.

13.2.11.1.2 – Agentes para endpoints - Coletas para investigação - Permitir a coleta de, no mínimo, as seguintes informações para investigação, sendo remoto ou não: - Arquivos copiados para dispositivos de armazenamento externo e vice-versa;

Resposta:
• Para haver coleta de informações de dados dos dispositivos plugados nas portas USB (dispositivo externo), o agente deve estar com comunicação plena com o servidor, sem bloqueios de portas ou protocolos, o que não foi observado. Não foi dado tempo para troubleshootig (análise e resolução de problemas) e a prova de conceito foi encerrada ANTES do tempo mínimo dado apenas para a instalação da solução.

13.2.11.1.3 - Agentes para endpoints - Coletas para investigação - Permitir a coleta de, no mínimo, as seguintes informações para investigação, sendo remoto ou não: - Falhas de logon e logoff;

Resposta:
• Para a realização deste teste, é imprescindível a plena comunicação dos agentes coletores com o servidor central,

o que foi impossibilitado pelas configurações de rede do cliente, que bloqueou as portas e/ou protocolos de comunicação necessários para o pleno funcionamento da solução. Houve pressão de tempo para a finalização da prova de conceito, a qual terminou bem antes do tempo mínimo dado em edital, apenas para a instalação da solução, o que impossibilitou que fossem realizadas ações de troubleshotting (resolução de problemas técnicos)

13.2.11.1.4 - Agentes para endpoints - Coletas para investigação - Permitir a coleta de, no mínimo, as seguintes informações para investigação, sendo remoto ou não: - Logins paralelos;

Resposta:
• Os logins paralelos ocorrem quando há a mesma conta de usuário logado em mais de um computador simultaneamente. Para que o sistema colete este tipo de informação, é imprescindível que os computadores monitorados pela solução se comuniquem sem bloqueios a portas e/ou protocolos.

13.2.11.1.5 - Agentes para endpoints - Coletas para investigação - Permitir a coleta de, no mínimo, as seguintes informações para investigação, sendo remoto ou não: - Tentativa de resolução de hostname;
Resposta:
• Demonstrado nas colunas no relatório em "nome do computador". Item devidamente cumprido pela empresa.

13.2.11.1.6 - Agentes para endpoints - Coletas para investigação - Permitir a coleta de, no mínimo, as seguintes informações para investigação, sendo remoto ou não: - Tentativa de acesso a URL;

Resposta:
• As tentativas de acesso à URL são catalogadas pelo sistema após alguns correlacionamentos, pelo servidor, executados a partir da coleta dos dados da estação de trabalho. Considerando que a coleta dos dados estava totalmente prejudicada pelo bloqueio de portas e/ou protocolos de comunicação e ainda considerando a falta de tempo hábil para a solução de problemas, o teste não foi executado, o que impossibilita decidir que a empresa desatende ao item.

13.2.11.1.7 - Agentes para endpoints - Coletas para investigação - Permitir a coleta de, no mínimo, as seguintes informações para investigação, sendo remoto ou não: - Logs do Windows com eventos de aplicação, segurança e sistema;

Resposta:
• A coleta de LOGs é realizada através dos agentes instalados na estação monitorada e, posteriormente enviada para o servidor, que processa os dados e faz os correlacionamentos. Como não havia comunicação entre os pontos envolvidos (estação e servidor), os logs não puderam ser enviados, da estação para o servidor, impossibilitando o teste. Não houve tempo hábil para a investigação e solução do problema.

13.2.11.1.8 - Agentes para endpoints - Coletas para investigação - Permitir a coleta de, no mínimo, as seguintes informações para investigação, sendo remoto ou não: - Identificação de acesso remoto via processos, IP e conexões internas ou externas etc.;

Resposta:
• A identificação dos acessos ocorre quando há acessos realizados, bem como quando há plena comunicação entre os pontos monitorados envolvidos na investigação. Não foi observada nenhuma das premissas citadas, impossibilitando o teste.

13.2.11.1.10 - Agentes para endpoints - Coletas para investigação - Permitir a coleta de, no mínimo, as seguintes informações para investigação, sendo remoto ou não: - Portas de rede ativas;

Resposta:
• O monitoramento de portas de rede só pode ser realizado quando há tráfego sem bloqueios de portas e/ou protocolos, o que não foi observado na prova de conceito.

13.3.6.10 – Sistema de Gerenciamento Centralizado – Segregação lógica - As comunicações efetuadas pelos processos analisados, por meio da listagem de conexões TCP/IP que foram efetuadas pelos sistemas e em que portas.

Resposta:
• O monitoramento de portas de rede só pode ser realizado quando há tráfego sem bloqueios de portas e/ou protocolos, o que não foi observado na prova de conceito.

13.3.11.15 - Sistema de Gerenciamento Centralizado – Relatórios - Informações de arquivos copiados dos discos locais dos endpoints para dispositivos de armazenamento externo e vice-versa;

Resposta:
• Para haver coleta de informações de dados dos dispositivos plugados nas portas USB, o agente deve estar com comunicação plena com o servidor, sem bloqueios de portas e/ou protocolos, o que não foi observado. Não foi dado tempo para troubleshootig (análise e resolução de problemas) e a prova de conceito toda foi encerrada ANTES do tempo mínimo dado apenas para a instalação da solução.

13.3.11.16 - Sistema de Gerenciamento Centralizado – Relatórios - Informações de histórico de ocorrências quanto ao uso simultâneo de redes WIFI e cabeadas por máquina ou por usuário;

Resposta:
• Não foi disponibilizado equipamento com conexão de rede sem fio (wifi) para evidenciação do solicitado em edital. Impossibilitando assim a decisão acerca do descumprimento do item por parte da empresa.

13.3.11.20 - Sistema de Gerenciamento Centralizado – Relatórios - Estatísticas da rede;

Resposta:
• Não é possível obter estatísticas de rede quando o tráfego está bloqueado, tanto por IP quanto por portas/protocolos. Não foi possível que o sistema realizasse a transferência dos dados coletados pelo agente para o servidor, que é responsável pela extração do relatório solicitado no item.

5. DA APTIDÃO OPERACIONAL DO SISTEMA

Como já mencionado, a licitação na modalidade pregão eletrônico, tinha por objeto a contratação de solução de cibersegurança, auditoria e prevenção de ameaças à base de dados não estruturados em endpoint.

O software de segurança a ser fornecido à PRODAM, que foi apresentado na Prova de Conceito – POC, em conformidade com as previsões do edital, é o sistema de segurança Loqed, que possui aptidão operacional já reconhecida em diversos órgãos estatais e empresas privadas, em diversos estados brasileiros

A exemplo da qualidade técnica do sistema fornecido, pode-se destacar três recentes atestados de capacidade técnica, inclusive um datado de 08 de fevereiro de 2023, emitidos por diferentes pessoas jurídicas, quais sejam:

• Datacheck – CyberSecurity, com sede na Avenida Cauaxi, 293 – Sala 2704 – Alphaville – SP. Fone: (11) 4195-6704
www.datacheck.com.br

• Secretaria de Estado da Administração do estado de Santa Catarina/SC – Gerência de Tecnologia da Informação e Governança Eletrônica. Fone: (48) 3665-1588.
Email: renato_deggau@sea.sc.gov.br

• Serviço Brasileiro de Apoio às Micro e Pequenas Empresas – SEBRAE, com sede no SGAS 605, Conjunto A, Asa Sul, Brasília/DF. Fone: 0800 570 0800. O Gerente da UTIC do Sebrae, Sr. Diego Almeida, e-mail diego.almeida@sebrae.com.br

Em especial atenção ao atestado de capacidade técnica emitido pela Datacheck – CyberSecurity, há a informação de que o início da parceria comercial com a empresa fornecedora do sistema de segurança iniciou em 01 de novembro de 2021 e se permeia ao longo dos anos até o presente momento com o serviço apresentando sempre alto nível de resultados.

Os demais contratos, representados pelos atestados de capacidade técnica, comprovam que o sistema operacional de segurança e cibersegurança fornecido por esta empresa recorrente (WAVEZ TECNOLOGIA E COMUNICAÇÃO DIGITAL LTDA.) possui ampla aptidão funcional.

Quaisquer adversidades que ocorreram na prova de conceito, nada se relaciona com a operacionalidade do software, que possui funcionalidade comprovada no mercado, em verdade, a rede de instalação disponibilizada na POC não estava apta para demonstração.

No ambiente de operação, o agente manda informação num intervalo temporal, dependendo do tipo de alerta - crítico, médio e informativo. O agente instalado na máquina final usa a rede interna do ambiente para se comunicar com a central, visualizando o IP do servidor, e a comunicação se dá via protocolo TCP/IP, com portas de rede específicas In/Out, na central e no endpoint. Se existir alguma falha de comunicação, entre o endpoint e a central, um serviço do agente no endpoint guarda a informação para envio, com temporizador para envio do alerta, tentando novamente de forma continuada.

Na produção, tudo o que acontece (problema de comunicação etc.) fica armazenado na central e no endpoint, para análise e reparo na configuração de rede.

Durante a prova de conceito, as máquinas que foram disponibilizadas estavam instalando/reinstalando programas básicos do Windows

Inclusive, para extirpar quaisquer dúvidas sobre a capacidade funcional do software Loqed, requer sejam feitas diligências nas empresas emissoras dos atestados de capacidade técnica acima mencionadas, que poderá comprovar a aptidão do sistema de segurança nos serviços oferecidos, conforme transcrito no tópico dos pedidos.

De modo sugestivo, para otimizar a diligência nos clientes, segue questionamentos a serem feitos aos clientes acima mencionados, acerca da operacionalidade técnica do Loqed:

1) O sistema funciona em endpoints com diversos sistemas operacionais, como Windows 7, Windows 28, Windows Server 2008, etc.?

2) Monitora arquivos manípulos em dispositivos USB, máquinas locais, arquivos compartilhados na rede?

3) Monitora comportamento do usuário?

4) Monitora processos maliciosos e em tempo real?

5) Faz análise de vulnerabilidade?

6) Monitora ações do usuário no endpoint, como: páginas web acessadas, downloads, uploads, uso de aplicativos, instalações de software, atividade de login e logoff?

7) Monitora drivers, serviços, e componentes do sistema operacional?

8) Demonstra todas as estatísticas de rede, como portas de rede, conexões, placa de rede, cabeamento?

6. DO PEDIDO

De todo o exposto, considerando os sólidos argumentos fáticos e jurídicos constantes da peça recursal, requer:

• sejam feitas diligências nas empresas emissoras dos atestados de capacidade técnica acima mencionadas, fato que poderá comprovar a aptidão do sistema de segurança nos serviços oferecidos;

• PROVIMENTO TOTAL AO RECURSO, REFORMANDO- SE A DECISÃO ALCANÇADA NO JULGAMENTO, a fim de OPORTUNIZAR NOVA DATA PARA REALIZAÇÃO DA POC – PROVA DE CONCEITO, e, após, comprovadas as diligências e preenchimento dos requisitos da prova de conceito, declare a Wavez Tecnologia como vencedora do certame.

Requer outrossim, a continuidade do certame, após o saneamento justo e necessário dos atos irregulares do procedimento, conforme aqui requeridos.

Termos em que pede e aguarda deferimento.

Brasília, 09 de fevereiro de 2023

Wavez Tecnologia e Comunicação Digital LTDA

Fechar