Gmail **Comissão Permanente de Licitação Docas do Ceara <cpl.docas@gmail.com>**

PEDIDO DE ESCLARECIMENTOS PREGÃO ELETRÔNICO Nº 022/2020

2 mensagens

Rafael Timbó <rafael.timbo@energytelecom.com.br> 19 de novembro de 2020 17:48
Para: "cpl.docas@gmail.com" <cpl.docas@gmail.com>
Cc: Darlan Rodrigues <darlan.rodrigues@energytelecom.com.br>

Boa tarde,

A CORESEC SEGURANÇA DA INFORMAÇÃO LTDA, inscrita no CNPJ nº 08.786.682/0001-11, vem através deste respeitosamente solicitar o esclarecimento abaixo acerca do PREGÃO ELETRÔNICO Nº 022/2020, conforme descrito abaixo:

1.2.11.10. Deve implementar Network Prefix Translation (NPTv6), prevenindo problemas de roteamento assimétrico;

O NPTv6 trata-se de uma implementação para redes internas IPv6, considerada inclusive experimentar, conforme RFC 6296 (https://tools.ietf.org/html/rfc6296#section-2.1),. Além do fator de ser uma versão experimental, entendemos que o cliente não utiliza, pelo menos plenamente, os recursos de IPv6. Dessa forma podemos considerar que este item não é obrigatório para o ambiente atual da Companhia Docas do Ceará. Está correto nosso entendimento?

1.2.25. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

Como trata-se da versão 3 do protocolo OSPF, somente para roteamento estático e ainda restrito para IPv6. Da mesma forma do item anterior, este requisito só teria sentido quando da utilização plena do protocolo IPv6 e com roteamentos estáticos, o que nem é recomendável haja vista a dinamicidade requerida nas soluções contemporâneas. Entendemos, portanto, que este item não é obrigatório para o ambiente atual da Companhia Docas do Ceará. Está correto nosso entendimento?

1.2.27.4. Associações de Segurança das VPNs;

Entendemos que há diversos mecanismos para garantir o conhecimento das sessões em caso de interrupção de um dos nós do cluster, assim como todo e qualquer tipo de conexões que estes mantenham. Portanto, o atendimento a estes pontos é opcional. Está correto nosso entendimento?

1.2.29. As funcionalidades de controle de aplicações, VPN IPSec e SSL, QOS, SSL e SSH Decryption e protocolos de roteamento dinâmico devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.

Entendemos que a funcionalidade de SSH Decryption não faz parte da demanda técnica do ambiente portanto, o atendimento a esta aplicação é opcional. Está correto nosso entendimento?

1.3.21. HTTP, FTP, SMB, SMTP, Telnet, SSH, MS-SQL, IMAP, IMAP, MS-RPC, RTSP e File body.

Entendemos que o reconhecimento de aplicações através de File body não é um recursos usual de redes modernas e mesmo de redes com configurações mais comuns, existindo outros mecanismos mais modernos. Dessa forma entendemos que este requisito não é obrigatório para o ambiente da Companhia Docas do Ceará. Está correto nosso entendimento?

1.4.26. Deve suportar varias técnicas de prevenção, incluindo Drop e tcp-rst (Cliente, Servidor e ambos);

Entendemos que as técnicas de prevenção DROP e RESET atendem a demanda técnica do ambiente. Está correto nosso entendimento?

1.4.30. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS e Antyspyware;

Entendems que a demanda de captura de pacotes pode ser realizada através de diversas ferramentas, e que sua realização através do equipamento de NGFW não faz parte da demanda do ambiente. Está correto nosso entendimento?

1.4.40. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e class), Android APKs, MacOS (mach-O, DMG e PKG), Linux (ELF), RAR e 7-ZIP no ambiente de sandbox;

Este item traz uma lista de tipos de arquivos que acaba limitando a participação de soluções de fabricantes amplamente reconhecidos no mercado que podem oferecer maior suporte nos requisitos de segurança. Neste sentido entendemos que soluções que consigam arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e class), DMG e PKG), Linux (ELF), e 7-ZIP no ambiente de sandbox atendem a este requisito. Está correto nosso entendimento?

1.4.42. Permitir o envio de arquivos e links para análise no ambiente controlado de forma automática via API.

Entendemos que este recurso só é necessário se o cliente tem algum tipo de solução de terceiros e/ou com desenvolvimento próprio que acesse as informações do firewall a partir de API. Dessa forma, entendemos que este requisito não é obrigatório para o pleno funcionamento do ambiente da Companhia Docas do Ceará.

Está certo nosso entendimento?

1.5.21. Deve salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: UserAgent, Referer, e X-Forwarded For;

Entendemos que este ítem é plenamente atendido quando a solução consegue salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: UserAgent e Referer. Está correto nosso entendimento?

1.6.2.11. Mac OS X 10.10 (Yosemite);

As versões 10.9 e 10.10 são versões mais antigas e que já perderam suporte do fabricante com relação a uma série de item. Por tanto, entendemos que o atendimento a eles é opcional. Está correto nosso entendimento?

1.6.18.3. Dispositivos Still Image como câmeras e Scanners;

1.6.18.4. Dispositivos de armazenamento CD, DVD RW;

Entendemos que o atendimento ao controle de acesso a dispositivos de armazenamento já obsoletos como CD e DVD RW, de dispositivos que correspondem a demanda técnica do ambiente como Still Image e Vmware USB Passthrough, é opcional. Está correto nosso entendimento?

1.6.20. Capacidade de extrair mais de 6 milhões de características dos arquivos potencialmente perigosos e aplicar algoritmos de análise para determinar sua intenção;

Entendemos que o número de 6 milhões de características pode ser obtido a partir do cruzamento de informações, bem como a utilização de mecanismos modernos de análises. Dessa forma não seria um item obrigatório a comprovação do número de 6 milhões, tendo em vista que o que importa é o resultado seguro das análises. Está correto nosso entendimento?

1.6.29.2. RAR;

1.6.29.6. WAR.

Entendemos que a análise de arquivos compactados WAR e RAR não faz parte da demanda técnica do ambiente. Está correto nosso entendimento?

1.6.48. Deve suportar a inclusão de certificados digitais para que arquivos assinados com estes certificados estejam dentro de uma lista segura (Safe List) para a execução;

Entendemos que o suporte a inclusão de certificados digitais para que arquivos assinados com estes certificados estejam dentro de uma lista segura (Safe List) para a execução não faz parte da demanda técnica do ambiente, e por isso o atendimento a este ponto é opcional. Está correto nosso entendimento?

Atenciosamente,

Comissão Permanente de Licitação Docas do Ceara <cpl.docas@gmail.com> 20 de novembro de 2020 17:30
Para: Rafael Timbó <rafael.timbo@energytelecom.com.br>

Boa tarde Rafael Timbó,

Com fulcro no item 24.2 do edital e conforme resposta emitida pela área técnica da CDC, segue, abaixo, as respostas quanto aos questionamentos suscitados.

1.2.11.10. Deve implementar Network Prefix Translation (NPTv6), prevenindo problemas de roteamento assimétrico;
O NPTv6 trata-se de uma implementação para redes internas IPv6, considerada inclusive experimentar, conforme RFC 6296 (https://tools.ietf.org/html/rfc6296#section-2.1),. Além do fator de ser uma versão experimental, entendemos que o cliente não utiliza, pelo menos plenamente, os recursos de IPv6.

Dessa forma podemos considerar que este item não é obrigatório para o ambiente atual da Companhia Docas do Ceará. Está correto nosso entendimento?
R: As redes que utilizam IPv6 no ambiente CDC, são, atualmente, todas internas. Todavia ainda que se trate de versão experimental, considerando que a contratação pretendida tem prazo de vigência de 05(cinco) anos, e que o protocolo IPv6 pode passar a ser padrão nesse período, é imprescindível que a solução apresentada disponha dessa funcionalidade.

1.2.25. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);
Como trata-se da versão 3 do protocolo OSPF, somente para roteamento estático e ainda restrito para IPv6. Da mesma forma do item anterior, este requisito só teria sentido quando da utilização plena do protocolo IPv6 e com roteamentos estáticos, o que nem é recomendável haja vista a dinamicidade requerida nas soluções contemporâneas. Entendemos, portanto, que este item não é obrigatório para o ambiente atual da Companhia Docas do Ceará. Está correto nosso entendimento?
R: Da mesma forma do item anterior, as redes que utilizam IPv6 no ambiente CDC, são, atualmente, todas internas. Todavia ainda que se trate de versão experimental, considerando que a contratação pretendida tem prazo de vigência de 05(cinco) anos, e que o protocolo IPv6 pode passar a ser padrão nesse período, é imprescindível que a solução apresentada disponha dessa funcionalidade.

1.2.27.4. Associações de Segurança das VPNs;
Entendemos que há diversos mecanismos para garantir o conhecimento das sessões em caso de interrupção de um dos nós do cluster, assim como todo e qualquer tipo de conexões que estes mantenham. Portanto, o atendimento a estes pontos é opcional. Está correto nosso entendimento?
R: SIM, o atendimento a este requisito é desejável, porém não imprescindível.

1.2.29. As funcionalidades de controle de aplicações, VPN IPSec e SSL, QOS, SSL e SSH Decryption e protocolos de roteamento dinâmico devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.
Entendemos que a funcionalidade de SSH Decryption não faz parte da demanda técnica do ambiente portanto, o atendimento a esta aplicação é opcional. Está correto nosso entendimento?
R: SIM, o atendimento a este requisito é desejável, porém não imprescindível..

1.3.21. HTTP, FTP, SMB, SMTP, Telnet, SSH, MS-SQL, IMAP, IMAP, MS-RPC, RTSP e File body.
Entendemos que o reconhecimento de aplicações através de File body não é um recursos usual de redes modernas e mesmo de redes com configurações mais comuns, existindo outros mecanismos mais modernos. Dessa forma entendemos que este requisito não é obrigatório para o ambiente da Companhia Docas do Ceará. Está correto nosso entendimento?
R: Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer estas aplicações, inclusive File Body, uma vez que não se pretende abrir mão de recursos de segurança.

1.4.26. Deve suportar varias técnicas de prevenção, incluindo Drop e tcp-rst (Cliente, Servidor e ambos);
Entendemos que as técnicas de prevenção DROP e RESET atendem a demanda técnica do ambiente. Está correto nosso entendimento?
R: SIM, as técnicas de Drop e Reset atendem à exigência, todavia, conforme apresentado no item, é imprescindível a inclusão da técnica de tcp-rst, de modo que se houver apenas as duas primeiras técnias presentes, mas não a tcp-rst, não será considerada cumprida a exigência.

1.4.30. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS e Antyspyware; ou outros filtros na solução
Entendemos que a demanda de captura de pacotes pode ser realizada através de diversas ferramentas, e que sua realização através do equipamento de NGFW não faz parte da demanda do ambiente. Está correto nosso entendimento?
R: Embora a captura de pacotes possa ser realizada através de diversas ferramentas, a utilização do equipamento NGFW se deve ao fato de ser um firewall capaz de oferecer os recursos mais avançados frente a novas ameaças constantes, para proteção das redes às quais ele gerencia. Os firewalls de última geração (NGFWs) são firewalls de inspeção profunda de pacotes que vão além da inspeção e bloqueio de portas / protocolos para adicionar inspeção no nível do aplicativo, prevenção de intrusões e trazer inteligência de fora do firewall. Um NGFW não deve ser confundido com um IPS (sistema de prevenção de intrusões de rede), que inclui um firewall comum ou não corporativo, ou um firewall e IPS no mesmo dispositivo que não está intimamente integrado.
Um Firewall tradicional atende às regras baseadas às camadas (1) Endereço de IP e (2) Porta, desta forma, as suas funções, ficam limitadas na Camada 3 (Redes) e Camada 4 (Transporte) do Modelo OSI. No NGFW é possível administrar através das demais camadas 5,6 e 7, que são as camadas de Aplicação do Modelo OSI, sendo pois imprescindível para esta contratação.

1.4.40. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e class), Android APKs, MacOS (mach-O, DMG e PKG), Linux (ELF), RAR e 7-ZIP no ambiente de sandbox;
Este item traz uma lista de tipos de arquivos que acaba limitando a participação de soluções de fabricantes amplamente reconhecidos no mercado que podem oferecer maior suporte nos requisitos de segurança. Neste sentido entendemos que soluções que consigam arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e class), DMG e PKG), Linux (ELF), e 7-ZIP no ambiente de sandbox atendem a este requisito. Está correto nosso entendimento?
R: Considerando que o número de ameaças de invasão aos sistemas de dados das companhias ou mesmo de órgãos do governo vem se intensificando e se tornando cada vez mais arrojadas, é importante adotar o máximo de medidas possíveis pra preservar a segurança dos ambientes de dados. Assim, A partir do momento em que os ataques cibernéticos se tornam mais sofisticados, monitorar comportamento suspeito se torna algo cada vez mais difícil. Muitas ameaças em anos recentes empregaram técnicas avançadas de evasão de detecção de firewall e soluções de segurança de rede.
O ambiente Sandbox protege a infraestrutura crítica de uma empresa de códigos suspeitos, porque funciona de forma segregada. Também permite que a segurança teste códigos maliciosos em um ambiente de testes isolado, para entender como é o comportamento desse código e detectar mais rapidamente ataques semelhantes.
No que tange especificamente às extenções Android APKs, MacOS (mach-O) e Linux(elf) remove-las do pacote de exigências das especificações implica necessariamente em abrir mão de camada extra de segurança em benefício do aumento de soluções a serem apresentadas na licitação, todavia com menor segurança, algo que não é aceitável.

1.4.42. Permitir o envio de arquivos e links para análise no ambiente controlado de forma automática via API.
Entendemos que este recurso só é necessário se o cliente tem algum tipo de solução de terceiros e/ou com desenvolvimento próprio que acesse as informações do firewall a partir de API. Dessa forma, entendemos que este requisito não é obrigatório para o pleno funcionamento do ambiente da Companhia Docas do Ceará. Está certo nosso entendimento?
R: NÃO. A Companhia dispõe de softwares com desenvolvimento próprio e em constante aprimoramento, de modo que o recurso para análise de links em ambiente controlado é uma ferramenta desejável para realização de testes seguros das aplicações.

1.5.21. Deve salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: UserAgent, Referer, e X-Forwarded For;
Entendemos que este ítem é plenamente atendido quando a solução consegue salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: UserAgent e Referer. Está correto nosso entendimento?
R: Sim, é suficiente.

1.6.2.11. Mac OS X 10.10 (Yosemite);
As versões 10.9 e 10.10 são versões mais antigas e que já perderam suporte do fabricante com relação a uma série de item. Por tanto, entendemos que o atendimento a eles é opcional. Está correto nosso entendimento?
R: SIM, por se tratar de versões mais antigas é opcional.

1.6.18.3. Dispositivos Still Image como câmeras e Scanners;
1.6.18.4. Dispositivos de armazenamento CD, DVD RW;
Entendemos que o atendimento ao controle de acesso a dispositivos de armazenamento já obsoletos como CD e DVD RW, de dispositivos que correspondem a demanda técnica do ambiente como Still Image e Vmware USB Passthrough, é opcional. Está correto nosso entendimento?
R: Por mais que o CD e DVD RW estejam praticamente sem uso, o parque de computadores da CDC dispõe de tais dispositivos instalados nos desktops e notebooks, de modo que se faz necessário controlar o acesso a estes dispositivos, bem como, os demais (Still Image e Vmware USB Passthrough).

1.6.20. Capacidade de extrair mais de 6 milhões de características dos arquivos potencialmente perigosos e aplicar algoritmos de análise para determinar sua intenção;
Entendemos que o número de 6 milhões de características pode ser obtido a partir do cruzamento de informações, bem como a utilização de mecanismos modernos de análises. Dessa forma não seria um item obrigatório a comprovação do número de 6 milhões, tendo em vista que o que importa é o resultado seguro das análises. Está correto nosso entendimento?
R: O número de 6 milhões de características pode ser obtido a partir do cruzamento de informações, bem como a utilização de mecanismos modernos de análises, porém é necessária a comprovação de que o cruzamento dessas informações ou utilização de mecanismos mais modernos possam extrair ao menos esse número de características ou mais.

1.6.29.2. RAR;
1.6.29.6. WAR.
Entendemos que a análise de arquivos compactados WAR e RAR não faz parte da demanda técnica do ambiente. Está correto nosso entendimento?
R: NÃO. Por se tratar de arquivos compactados, os mesmos podem conter arquivos de código malicioso, trazendo risco à Companhia.

1.6.48. Deve suportar a inclusão de certificados digitais para que arquivos assinados com estes certificados estejam dentro de uma lista segura (Safe List) para a execução;
Entendemos que o suporte a inclusão de certificados digitais para que arquivos assinados com estes certificados estejam dentro de uma lista segura (Safe List) para a execução não faz parte da demanda técnica do ambiente, e por isso o atendimento a este ponto é opcional. Está correto nosso entendimento?
R: NÃO, a funcionalidade de criação de safe list para inclusão de certificados cuja verificação garantam sua segurança é fundamental haja vista que a solução de gestão de processos da CDC pode utilizar assinaturas por certificados e tal ferramenta garantirá segurança na verificação dos arquivos anexados bem como da documentação recebida por outros órgãos externos.

Respeitosamente,

Dra. Roberta Siebra
Pregoeira da Comissão Permanente de Licitação.
COMPANHIA DOCAS DO CEARÁ.