PREFEITURA DE VILA VELHA

DESPACHO

PREGÃO ELETRÔNICO Nº: 119/2021

PROCESSO ADMINISTRATIVO Nº: 17368/2021

OBJETO: REGISTRO DE PREÇOS PARA CONTRATAÇÃO DE SOLUÇÕES DE SEGURANÇA DO TIPO ENDPOINT PROTECTION (ANTIVÍRUS) E DE GATEWAY DE E-MAIL (ANTISPAM), INCLUINDO SERVIÇOS DE INSTALAÇÃO, CONSOLE DE GERENCIAMENTO, SUPORTE TÉCNICO ON SITE, GARANTIA E ATUALIZAÇÃO POR 36 (TRINTA E SEIS) MESES

Vieram os autos a esta subsecretaria para fins de análise e parecer acerca dos aspectos técnicos, proposta comercial e demais exigência do Termo de Referência, conforme se observa do despacho de evento nº 50.

Após análise detida da documentação encaminhada pela empresa NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA, atual arrematante do certame, verificamos que a solução proposta não atende às seguintes exigências/requisitos do Termo de Referência:

Soluções da Kapersky e Fortigate que foram ofertadas:

Item	Descrição do Objeto	MARCA/ MODELO	UND	QTD	VALOR UNIT R$	VALOR TOTAL R$
01	Código PMVV: 6.06.14.0199.3 Serviço de Licenciamento de uso da solução de software Antivírus com atualização continuada, conforme especificações contidas em Termo de Referência – Endpoints (Desktop).	Fabricante: Kaspersky Lab. Versão: Kaspersky Endpoint Security for Business Advanced 36 meses	UND	5.715	R$ 162,00	R$ 925.830,00
02	Código PMVV: 6.06.14.0200.0 Serviço de Licenciamento de usoda solução de software Antivírus com atualização continuada, conforme especificações contidas em Termo de Referência – Endpoints (Servidores).	Fabricante: Kaspersky Lab. Versão:Kaspersky Endpoint Security for Business Advanced 36 meses	UND	250	R$ 180,00	R$ 45.000,00
03	Código PMVV: 6.06.14.0201.9 Licenciamento de uso da solução de AntiSpam com atualização continuada, conforme especificações contidas em Termo de Referência.	Fabricante: Fortinet Versão: FortiMail Cloud Gateway Premium 36 Meses	UND	5.715	R$ 230,00	R$ 1.314.450,00
04	Código PMVV: 6.07.38.0096.0 Serviço de implementação, configuração e transferência de conhecimento para solução de Endpoints (Desktop)	-	SERV	3	R$ 31.000,00	R$ 93.000,00
05	Código PMVV: 6.07.38.0097.9 Serviço de implementação, configuração e	-	SERV	3	R$ 4.500,00	R$ 13.500,00

Documentações utilizadas:

https://media.kaspersky.com/br/business-security/kaspersky-endpoint-security-for-business-datasheet.pdf

https://support.kaspersky.com/KESWin/11.7.0/pt-BR/127971.htm

https://support.kaspersky.com/KESWin/11.7.0/pt-BR/176745.htm

https://support.kaspersky.com/KSC/11/en-US/151324.htm

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiMail-Cloud-Gateway.pdf

https://docs.fortinet.com/document/fortimail/7.0.1/administration-guide/313415/email-concepts-and-process-workflow

Segue abaixo os itens descritos no edital que não foram identificados na documentação pública dos fabricantes supra citados.

2.2.1 ITEM 01 - SOLUÇÃO DE SEGURANÇA DO TIPO ENDPOINT PROTECTION (ANTIVÍRUS)

2.2.1.1.3. A solução deve contemplar proteção contra-ataques: direcionados e suas variantes, 0Day (dia zero), vulnerabilidades desconhecidas ou novas, tais como as que possam causar estouro de buffer, ataques iniciados a partir de mídias removíveis, proteção contra BOT's e variantes, e ainda ter tecnologia de análise de comportamentos suspeitos para detecção e eliminação de ameaças desconhecidas.

A ferramenta que protege contra-ataques direcionados, ameaças persistentes avançadas (APT) e ataques de dia zero parece ser uma solução apartada do Endpoint Security.

https://support.kaspersky.com/KESWin/11.7.0/pt-BR/176745.htm

2.2.1.1.6. Monitoramento de atividades de criptografia de arquivos para evitar ataques de ransomware ou similar.

Não foi encontrada na documentação da solução nenhuma informação referente ao item acima.

2.2.1.1.7. Mitigação da Exploração de Memória (Memory Exploit Mitigation) ou similar

A solução não analisa processos em memória.

2 2.2.1.1.9. A solução deve ter a capacidade de impedir os ataques direcionados mesmo que utilizando as vulnerabilidades de 0Day (dia zero), mitigando no mínimo os conhecidos comportamentos de exploração de vulnerabilidades a seguir: a) SEHOP - Structured Exception Handler Overwrite Protection ou similar; b) Heap Spray (Exploits que iniciam através do HEAP) ou similar; c) Java Exploit Protection;

Não foi encontrada na documentação da solução nenhuma informação referente ao item acima.

2.2.1.1.10. A solução deve ter a capacidade de bloquear exploits que trabalham em nível de "shell code" e suas variantes, assim como, implementar a funcionalidade de "virtual patching" ou qualquer outra técnica para blindagem para aplicações, sistemas e sistemas operacionais contra exploração de vulnerabilidades conhecidas.

A solução não realiza virtual patching para a proteção de sistemas operacionais e aplicações.

2.2.1.1.12. A solução deve ter a capacidade de receber instruções de comando contra ataques de APT (Ameaça Persistente Avançada) ou similar, sem a necessidade de interpretação pelo gerenciador do endpoint, possibilitando ações mais rápidas, assertivas e minimizando falsos positivos.

Não foi encontrada na documentação da solução nenhuma informação referente ao item acima. A ferramenta que protege contra ameaças persistentes avançadas (APT) e ataques de dia zero parece ser uma solução apartada do Endpoint Security.

https://support.kaspersky.com/KESWin/11.7.0/pt-BR/176745.htm

2.2.1.1.19. Permitir configurar quais tipos de arquivos serão verificados (ex: arquivos comprimidos, arquivos auto descompactáveis, .PST, arquivos compactados por compactadores binários, executáveis, cab, msi e outros).

2.2.1.1.25. Possibilidade de criar uma cópia backup do arquivo suspeito antes de qualquer ação.

2.2.1.1.26. Possibilitar a criação de uma imagem para verificação e remoção de ameaças sem a necessidade de carregar o Sistema Operacional.

2.2.1.1.27. Capacidade de limitar o acesso dos sistemas e aplicativos a recursos do sistema operacional, como chaves do registro e pastas e arquivos, em casos de falha, permitir a limpeza de chaves e pastas.

Não foi encontrada na documentação da solução nenhuma informação referente aos itens acima.

2.2.1.1.28. Detecção Proativa de reconhecimento de novas ameaças.

A ferramenta que protege contra-ataques direcionados, ameaças persistentes avançadas (APT) e ataques de dia zero parece ser uma solução apartada do Endpoint Security.

https://support.kaspersky.com/KESWin/11.7.0/pt-BR/176745.htm

2.2.1.1.30. Deve ter a possibilidade de notificação customizada para o usuário com diferentes ícones.

A solução não possui funcionalidade de customização de ícones de notificação.

https://support.kaspersky.com/KESWin/11.7.0/pt-BR/130890.htm

2.2.1.1.38. A solução deverá possuir rotinas bem definidas de escaneamento, atualizações e de logs.

2.2.1.1.47. Deve ser capaz de detectar tentativas de mascaramento, evasão de detecção através do uso de portas comuns, tentativas de scan de rede, ataque de força bruta ou tunelamento de protocolos.

Não foi encontrada na documentação da solução nenhuma informação referente ao item acima.

2.2.1.2.15.A solução deverá ser compatível com sistemas operacionais: Windows 7 (32 e 64 bits) e superiores, MacOS (OS X 10.7 e superiores) nas versões (32 e 64 bits) e Linux (Ubuntu e suas variantes);

A Solução ofertada não oferece suporte a MacOS OS X 10.7

https://support.kaspersky.com/KESMac/11.2_adminguide/en-US/118665.htm

2.2.1.2.19. Possuir funcionalidades, inclusive recursivo em vários níveis, que permitam a detecção e reparo de arquivos contaminados por códigos maliciosos mesmo que sejam compactados.

2.2.1.2.22. A solução deve ser capaz de identificar e bloquear informações independente do meio de transmissão.

Não foi encontrada na documentação da solução nenhuma informação referente ao item acima.

2.2.2 ITEM 02 - SOLUÇÃO DE SOFTWARE ANTIVÍRUS - ENDPOINTS (SERVIDORES)

2.2.2.1.1. Possuir a capacidade de detectar mudanças de integridade em arquivos e diretórios do S.O. e aplicações terceiras.

Não foi encontrada na documentação da solução nenhuma informação referente a detecção de mudança de integridade em diretórios do S.O.

2.2.2.1.3. Possuir a capacidade de criação de regras de monitoramento em chaves de registro, diretórios e subdiretórios e, customização para criação de regras avançadas.

2.2.2.1.5. A solução deve possuir funcionalidades de otimização de verificação (escaneamento) em ambientes virtuais.

2.2.2.1.6. A solução deve permitir visualizar máquinas físicas e virtuais, possibilitando aplicar regras específicas para as máquinas virtuais.

2.2.2.1.9. Possuir a capacidade de varrer o sistema operacional e aplicações, recomendando regras de monitoramento de acordo com o resultado desta varredura;

2.2.2.1.13. Permitir que o administrador do sistema tenha a possibilidade de não aplicar automaticamente a proteção para as vulnerabilidades escolhendo o perfil ou o host.

2.2.2.1.14. Proteger de forma automática e transparente contra brechas de segurança descobertas interrompendo somente o tráfego malicioso.

2.2.2.1.15. Possuir a capacidade de detectar e bloquear ataques em aplicações web tais como: SQL Injection e Cross-Site Scripting dentre outros.

Não foi encontrada na documentação da solução nenhuma informação referente ao item acima.

2.2.2.1.16. O software de proteção deve ter a capacidade de bloquear exploits que trabalham em nível de "shell code", assim como, implementar a funcionalidade de "virtual patching" ou qualquer outra técnica para blindagem de sistemas e aplicações contra exploração de vulnerabilidades conhecidas.

Kaspersky para endpoint não realiza virtual patching para a proteção de sistemas operacionais e aplicações.

2.2.2.1.17. Implementar a customização avançada e criação de novas regras de proteção de aplicações web, permitindo proteger contra vulnerabilidades específicas de sistemas web da CONTRATANTE, inclusive sistemas legados.

2.2.2.1.20. Permitir que as regras de Firewall executem as seguintes ações, ou equivalentes: Allow, Log Only, bypass, force allow, deny.

2.2.2.1.21. Permitir limitar o número de conexões entrantes e de saída de um determinado IP de origem.

2.2.2.1.23. Possuir a capacidade de varrer o servidor protegido detectando o tipo e versão do S.O. e demais aplicações, recomendando ações para blindagem de vulnerabilidades existentes no S.O. e

2.2.2.1.28. Possuir a capacidade de armazenamento do pacote capturado quando detectado um ataque.

2.2.2.1.29. Possibilitar a criação de regras customizadas, para proteger aplicações desenvolvidas pela CONTRATANTE.

2.2.2.2.3. A solução deve ter a capacidade de implementar integração entre a gerência central com plataformas de terceiros (ferramentas para BI, por exemplo).

Não foi encontrada na documentação da solução nenhuma informação referente aos itens acima.

2.2.2.2.5. A solução deve possibilitar a criação de dashboards personalizados e permitir a exportação para, no mínimo, os formatos PDF, HTML, CSV ou TXT.

A solução não fornece opção para customização de Dashboards.

A solução não exporta para CSV ou TXT.

https://support.kaspersky.com/KSC/CloudConsole/en-US/176430.htm

2.2.2.2.7. Deverá permitir configuração de ações para arquivos infectados com console de interface gráfica intuitiva para que o administrador configure qual ação o Sistema tomará para arquivos infectados:

c) Limpar sem backup;

d) Excluir arquivo infectado;

2.2.2.2.40. Permitir configurar o consumo de recursos que será utilizado para varreduras.

2.2.2.2.44. Permitir configuração de regras de IDS/IPS diferenciadas de acordo com horário ou dia da semana.

2.2.2.2.49. Capacidade de oferecer informações para análise forense de artefatos suspeitos de serem maliciosos.

2.2.2.2.52. A solução deve possibilitar o envio de arquivos da área de isolamento para criação de vacinas automaticamente, permitindo o envio via protocolo seguro. Onde este será submetido ao fabricante da solução, sob responsabilidade e supervisão da Contratada.

Não foi encontrada na documentação da solução nenhuma informação referente aos itens acima.

ITEM 03 - SERVIÇO DE LICENCIAMENTO DE USO DA SOLUÇÃO DE ANTISPAM COM ATUALIZAÇÃO CONTINUADA

2.2.3.4. Controle de sessões SMTP por meio de limite de tráfego de mensagens baseado em endereços IP, sub-redes IP, domínio e reputação do emissor.

2.2.3.5. Inspeção e bloqueio de mensagens baseados em tamanho de mensagem, volume de mensagens por período, número de destinatários por mensagem, número de destinatários por hora, destinatários inválidos, número de mensagens por conexão e número de conexões simultâneas por endereço IP.

2.2.3.10. Implementação de recursos de controle de taxa, limitando a quantidade de e-mail aceitos de um emissor específico durante um período de tempo.

2.2.3.12. Filtragem de conteúdo de e-mails por meio de assinaturas para corpo e anexos de mensagens, heurística, filtro de reputação, URL's e filtros anti-phishing.

2.2.3.15. Categorização de mensagens de saída a partir de políticas preestabelecidas.

2.2.3.36. Deve possuir e utilizar filtros de reputação.

2.2.3.37. Deve ter a capacidade de implementar pesquisas de reputação, informando seu histórico de reputação, assim como, sua reputação atual.

2.2.3.38. Deve ter a capacidade de fazer filtragem do remetente a partir de uma correlação da reputação global, informada pelo fabricante do produto, em conjunto com a reputação local, restringindo conexões indesejadas.

2.2.3.42. A solução deverá possuir um sistema que permita estabelecer uma reputação (pontuação) dos endereços IP de servidores que estarão iniciando conexões TCP. Após estabelecida essa reputação, a solução deverá permitir ações diferenciadas de acordo com a pontuação obtida.

2.2.3.43. O administrador deverá ter a possibilidade de aplicar políticas por meio de pontuação podendo aplicar ações.

2.2.3.47. Possuir recurso capaz de deferir a conexão SMTP caso a fonte emissora tenha enviado um percentual de mensagens consideradas como SPAM, em um determinado espaço de tempo, ambos configuráveis pelo administrador.

2.2.3.57. A solução deverá possibilitar a configuração do período em que as mensagens ficarão em quarentena e após esse período as mensagens serão apagadas automaticamente.

Não foi encontrada na documentação da solução nenhuma informação referente aos itens acima.

2.2.3.60.5. A solução deve possibilitar a monitoração e geração de relatórios a partir da console de administração nos formatos PDF, HTML, CSV ou TXT, com a possibilidade de envio por email.

Para a extração de relatórios em todos os formatos especificados é necessário possuir também a solução FortiAnalyzer, que não foi ofertado na proposta em análise.

https://docs.fortinet.com/document/fortianalyzer/7.0.2/administration-guide/435266/viewing-completed-reports

https://docs.fortinet.com/document/fortimail/7.0.1/administration-guide/515570/viewing-generated-reports

2.2.3.60.10. Gerenciamento com recurso de auditoria de alteração de configurações e acesso à ferramenta de administração, incluindo usuário, data e horário de acesso e ações realizadas.

Identificado que o recurso de auditoria está presente apenas na solução FortiAnalyzer, que não foi ofertado na proposta em análise.

2.2.3.60.16. A solução deverá fornecer relatórios nos formatos PDF, HTML, CSV ou TXT, com a possibilidade de envio por e-mail.

Para a extração de relatórios em todos os formatos especificados é necessário possuir também a solução FortiAnalyzer, que não foi ofertado na proposta em análise.

https://docs.fortinet.com/document/fortianalyzer/7.0.2/administration-guide/435266/viewing-completed-reports

2.2.3.60.25. Notificar os administradores por e-mail caso a solução não receba atualizações por um determinado período de tempo.

Não foi encontrada na documentação da solução nenhuma informação referente ao item acima.

Oportuno registrar que, antes de deliberar pela desclassificação da proponente, realizamos diligências em sites, cujas fontes foram indicadas acima. Desta forma, considerando que a solução proposta não atende aos requisitos mínimos exigidos no instrumento convocatório, opinamos pela **DESCLASSIFICAÇÃO** da empresa **NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA**.

Vila Velha, 05/11/2021.

Hugo Ferreira Coelho
Subsecretário de Infraestrutura