Brasília/DF, 14 de março de 2008.

À
Controladoria Geral da União - CGU

Att.: Sr.(a). Pregoeiro (a);

Ref.: Pregão Eletrônico nº 02/2008

Prezado (a) Senhor(a):

A NCT Informática Ltda., portadora do CNPJ n° 03.017.428/0001-35, tendo analisado o Edital da licitação supra citada, vem diante desta Douta CPL, apresentar o questionamento conforme se segue:

Solicitamos esclarecimento sobre a participação de soluções similares em atendimento do objeto, resguardadas as funcionalidades e capacidades do equipamento existente, conforme especificação abaixo, praticando modalidade upgrade competitivo (fornecimento de equipamento novo, instalação e treinamento para 6 pessoas ao preço da renovação).

1. Capacidade de permitir, em caso de falha de hardware, a passagem de tráfego no segmento de rede sem afetar o funcionamento da rede;
2. Capacidade de monitoração de segmentos de rede em modo promíscuo, sem endereço IP, analisando cabeçalho (header) e área de dados (payload) dos pacotes que trafegam em rede, detectando ataques ou tráfego não autorizado ou suspeito;
3. Capacidade de implementação não intrusiva (Não é necessário a configuração de routers ou switches para sua instalação);
4. Capacidade de execução de bloqueio simulado nos seguintes modos:
    a. Funcionamento em linha, porém sem bloqueio dos ataques;
    b. Alerta de eventos que seriam bloqueados;
    c. Configuração de modo simulado para todo o tráfego ou apenas para pacotes especificados por endereço IP, protocolo e VLAN ID;
5. Funcionamento como equipamento de camada 2 (modelo OSI), permitindo a criação de regras para as camadas superiores do modelo OSI;
6. Possuir capacidade de criação de regras de firewall;
7. Funcionamento passivo como IDS (sistema de detecção de intrusos), com alertas de eventos de ataques, tráfego malicioso ou indesejado, sem interferência com o tráfego;
8. A combinação das modalidades IDS (passivo) e IPS (em linha) dentro de um mesmo equipamento. Todas as portas devem poder operar como IDS (passivo) ou IPS (em linha), permitindo operação das duas modalidades no mesmo equipamento e em portas diferentes;
9. Capacidade de identificar e bloquear tráfego de aplicações instante mensagens e P2P com suporte mínimos às aplicações abaixo:
    a. AOL Instant Messenger;
    b. MSN Messenger;
    c. Yahoo! Messenger;
    d. ICQ;
    e. Gnutella;
    f. Kazaa;
    g. eDonkey;
    h. BitTorrent;

i. SoulSeek;
j. DirectConnect;

10. Ter no mínimo 8 interfaces de 1 Gbps par trançado, com um throughtput de 1 Gbps para análise do tráfego;
11. Ter no mínimo uma interface 100 Mbps para comunicação com o sistema de administração;
12. Ter suporte a montagem em “rack 19”;
13. Atualização automática das “assinaturas” através de download seguro via Web;
14. Redundância de armazenamento com tolerância a falha, redundância nos ventiladores internos e fonte a fim de recuperar falhas graves no hardware e sem perda de log’s;
15. Capacidade, em caso de falha de hardware a passagem de tráfego no segmento de rede sem afetar o funcionamento da rede;
16. Alta-disponibilidade ativo-passivo;
17. Implementar inspeção do tipo “Deep Packet Inspection”;
18. Capacidade de remontagem da inspeção dos pacotes analisados;
19. Alta-disponibilidade ativo-ativo;
20. Monitoração de VLANs, incluindo frames 802.1q;
21. Capacidade de monitoração stateful inspection;
22. Detectar ataques independente do sistema operacional alvo;
23. Identificar o protocolo a partir da porta utilizada;
24. Identificar protocolos que utilizam portas aleatórias;
25. Identificar protocolo independente da porta utilizada;
26. Identificar protocolos mesmo quando encapsulados, exceto se o mesmo estiver em canal criptografado;
27. Analisar protocolos com decodificação mínima de 30 protocolos e formatos de dados nas 7 camadas OSI, permitindo a detecção de ataques desconhecidos ou variantes de ataques sem atualização das assinaturas. O fornecedor deve fornecer lista dos protocolos decodificados para a homologação;
28. Detectar a varreduras de portas;
29. Assinaturas baseadas em vulnerabilidades permitindo a detecção de ataques desconhecidos ou variantes de ataques;
30. Identificar anomalias de protocolo;
31. Identificar ataques de SYN Flood;
32. Suportar fragmentação e defragmentação IP;
33. Criar assinaturas definidas pelo usuário com uso de expressões regulares;
34. Criar regras baseadas em de segmento monitorado, ou seja, no equipamento ser possível aplicar diferentes políticas para diferentes segmentos;
35. Criar regras baseadas em endereço IP origem e destino;
36. Criar regras baseadas em portas IP origem e destino;
37. Capacidade de criar regras baseadas em VLAN ID;
38. Alterar formas de bloqueio individualmente para as assinaturas;
39. Filtros de protocolos TCP, UDP, ICMP;
40. Filtro de ataques específicos ou todos os ataques a partir de endereços/faixa IP específicos;
41. Resetar, dropar a sessão TCP quando utilizado em modo passivo;
42. Descarte de pacotes, como:
    a. Descartar todos os pacotes da conexão na qual o evento ocorreu e envia pacotes de reset TCP para origem e destino da conexão;
    b. Descarte de todos os pacotes da conexão na qual o evento ocorreu;
    c. Efetuar drop do pacote identificado com o ataque;

43. Neutralizar trojan – isolar código malicioso que está contido dentro de código aparentemente inofensivo;
44. Enviar de SNMP trap;
45. Enviar e-mail;
46. Resposta definida pelo usuário;
47. Possuir atualizações de assinaturas de forma dinâmica e automática quando estas estiverem disponíveis pelo fabricante, sem a necessidade de pesquisa de conteúdo de segurança para a atualização do produto;
48. Console gráfica local com possibilidade de acesso remoto;
49. Administração centralizada com interface gráfica;
50. Ajuste dinâmico de severidade de ataques, como resultado da correlação de eventos;
51. Capacidade de análise de vulnerabilidades;
52. Correlação de padrões de ataques (múltiplos eventos identificados como um único ataque);
53. Comunicação de dados criptografados;
54. Capacidade de geração de relatórios múltiplos;
55. Gerar sumários de relatórios das atividades registradas;
56. Textos e gráficos aleatórios, com exportação nos formatos HTML, PDF e CSV;
57. Console remota com interface gráfica;
58. Console remota web com interface gráfica para consulta;
59. Utilizar diferentes perfis de usuários;
60. Auditoria das atividades dos usuários;
61. Agendamento de tarefas;
62. Envio de eventos SNMP relativos ao desempenho e funcionamento do equipamento.

Sem mais,

Atenciosamente.

Núbia Leles de Oliveira
Departamento de Licitações
NCT Informática Ltda