PREFEITURA MUNICIPAL DE BELÉM
COMPANHIA DE INFORMÁTICA DE BELÉM – CINBESA
DIRETORIA DE TECNOLOGIA

JUSTIFICATIVA TÉCNICA

Na segunda metade do mês de Julho de 2014, a Cinbesa teve o acesso aos seus serviços publicados na Internet, prejudicado por ataques cibernéticos de origens não identificadas. Esses ataques foram do tipo DDOS, os quais obstruíram o canal de comunicação (link de Internet), impossibilitando o acesso aos sistemas. Em nenhum momento ocorreu invasão aos sistemas.

Devido esses constantes ataques DDOS aos endereços IP da CINBESA, urge a necessidade de imediata contratação do serviço de proteção contra esse tipo de ataque malicioso. Atualmente, o serviço de internet é provido pela operadora Embratel, que também é a única a oferecer esse serviço em Belém. Além do mais, esta proteção deve ser configurada no próprio Backbone do fornecedor do link Internet, impossibilitando que outra operadora forneça o serviço.

Para garantir proteção contra ataques DDOS, o fornecedor deverá disponibilizar em seu Backbone a proteção contra ataques de negação de serviços, evitando assim a saturação/congestionamento da banda contratada da Internet e a indisponibilidade dos serviços em momentos de ataques tanto DOS (origem única) e DDOS (origem múltipla) considerando os requisitos mínimos a seguir:

1. Serviços deverão ter pró-atividade para solução e prevenção de incidentes e ataques;
2. Monitorar disponibilidade e performance de todos os links de dados existentes nesse termo de referência em regime 24x7, utilizando profissionais de forma dedicada;
3. Tomar todas as providências necessárias para recompor a disponibilidade do link em caso de incidentes de ataques, recuperando o pleno funcionamento do mesmo pela contratada;

FLS. Nº 04
PROC. Nº 389
DATA: 07 / 08 / 14
ASS.

4. Solução deve possuir a capacidade de criar e analisar a reputação de endereços IP, possuindo base de informações própria, gerada durante a filtragem de ataques e interligada com os principais centros mundiais de avaliação de reputação de endereços IP;
5. A solução deve suportar a mitigação automática de ataques, utilizando múltiplas técnicas como White Lists, Black Lists, limitação de taxa, técnicas desafio-resposta, descarte de pacotes mal formados, técnicas de mitigação de ataques aos protocolos HTTP e DNS, bloqueio por localização geográfica de endereços IP, dentre outras;
6. A solução deve implementar mecanismos capazes de detectar e mitigar todos e quaisquer ataques que façam o uso não autorizado de recursos de rede, incluindo, mas não se restringindo aos seguintes:

   - ✓ Ataques de inundação (Bandwidth Flood), incluindo Flood de UDP e ICMP;
   - ✓ Ataques à pilha TCP, incluindo mal uso das Flags TCP, ataques de RST e FIN, SYN Flood e TCP Idle Resets;
   - ✓ Ataques que utilizam Fragmentação de pacotes, incluindo pacotes IP, TCP e UDP;
   - ✓ Ataques de Botnets, Worms e ataques que utilizam falsificação de endereços IP origem (IP Spoofing);
   - ✓ Ataques à camada de aplicação, incluindo protocolos HTTP e DNS;

7. A solução deve manter uma lista dinâmica de endereços IP bloqueados, retirando dessa lista os endereços que não enviarem mais requisições maliciosas após um período de tempo considerado seguro pelo fornecedor;
8. O fornecedor deverá possuir dois centros de limpeza nacional cada um com capacidade de mitigação de 1GB, centro de limpeza internacional com capacidade de mitigação de 30GB;

9. A contratada deve mitigar ataques por 3 horas, caso o ataque ultrapasse o SLA de mitigação contratado;
10. Caso o volume de tráfego do ataque ultrapasse as capacidades de mitigação especificadas ou sature as conexões do AS devem ser tomadas contramedidas tais como aquelas que permitam o bloqueio seletivo por blocos de IP de origem no AS pelo qual o ataque esteja ocorrendo, utilizando técnicas como Remote Triggered Black Hole;
11. As soluções de detecção e mitigação devem possuir serviço de atualização de assinaturas de ataques;
12. O fornecedor deve disponibilizar um Centro Operacional de Segurança (ou SOC – Security Operations Center) no Brasil, com equipe especializada em monitoramento, detecção e mitigação de ataques, com opção de atendimento através de telefone 0800, correio eletrônico, em idioma português brasileiro, durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual;
13. A mitigação de ataques deve ser baseada em arquitetura na qual há o desvio de tráfego suspeito comandado pelo equipamento de monitoramento, por meio de alterações do plano de roteamento;
14. Em momentos de ataques DOS e DDOS, todo trafego limpo deve ser injetado novamente na infraestrutura da contratante através de túneis GRE (Generic Routing Encapsulation), configurado entre a plataforma de DOS e DDOS do fornecedor e o CPE da CINBESA;
15. Para minimizar a possibilidade de espionagem, na mitigação dos ataques não será permitido o encaminhamento do tráfego para limpeza fora do território brasileiro;
16. As funcionalidades de monitoramento, detecção e mitigação de ataques devem ser mantidas em operação ininterrupta durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual;

17. Em nenhum caso será aceito bloqueio de ataques de DOS e DDOS por ACLs em roteadores de bordas do fornecedor;
18. O fornecedor deverá possuir um contrato SLA de 15 minutos para iniciar a mitigação de ataques de DDOS;
19. O fornecedor deverá disponibilizar uma Solução de Monitoração de acompanhamento contra ataques DDoS, que contemple:

- ✓ Quadro Sinóptico para visualização da ocupação de banda do link Internet e níveis de severidade dos ataques;
- ✓ Os alertas, que deverão fornecer, no mínimo, as seguintes funcionalidades:

  - Visualização de informações on-line, de forma gráfica da banda consumida no ataque;
  - Acompanhamento do nível de importância do ataque, o percentual do nível de severidade do ataque, o consumo de banda do ataque e tipo do ataque e classificação;
  - Origem de ataques com identificação do endereço IP e porta de origem;
  - Destino de ataques, com identificação do endereço IP e porta de destino;
  - Protocolo de transporte do alerta;
  - Cada alerta deverá ter um número de identificação que facilite sua consulta;
  - Informar a data de início e fim do acompanhamento do alerta;
  - Volume de ataques sumarizados por hora, dia, semana e mês;
  - Relatório por tipos de ataques;

FLS. Nº 07
PROC. Nº 389
DATA: 07 / 08 / 14
ASS.

PREFEITURA MUNICIPAL DE BELÉM
COMPANHIA DE INFORMÁTICA DE BELÉM – CINBESA
DIRETORIA DE TECNOLOGIA

- ✓ O Portal de Monitoração do fornecedor deverá possuir uma interface única para acesso às suas funcionalidades, independentemente dos equipamentos ou tecnologias empregadas para a prestação dos serviços;
- ✓ O Portal de Gerência deverá permitir o acesso simultâneo a, pelo menos, um administrador de rede da Cinbesa;

Desta forma estaremos protegendo o serviço de internet contra os ataques cada vez mais comum de DOS e DDOS, evitando que os serviços prestados pela CINBESA fiquem indisponíveis como ocorreu no último mês de julho.

Belém, 07 de Agosto de 2014.

Osman Bentes de Melo e Silva
Coordenador do Suporte Técnico- DT/CINBESA