Normas de Acordo Mútuo para Segurança de Roteamento

Mutually Agreed Norms for Routing Security (MANRS)

Introdução

Segurança, em geral, é uma área difícil e desafiadora. A segurança da infraestrutura de Internet global, seja a resolução de nomes de domínio (DNS) ou o roteamento, traz desafios adicionais: os resultados das medidas de segurança dependem de ações coordenadas dos participantes da rede.

Ao longo da história da Internet, a colaboração entre os participantes e a divisão de responsabilidades na sua operação têm sido dois dos pilares que suportam seu tremendo crescimento e sucesso, bem como sua segurança e resiliência. Soluções tecnológicas são elementos essenciais, mas a tecnologia sozinha não é suficiente. Para estimular melhorias significativas nessa área é necessária uma grande mudança em direção à cultura da responsabilidade coletiva.

Este documento visa incentivar esse espírito colaborativo e fornecer orientações para os operadores de rede na abordagem de questões de segurança e resiliência do sistema de roteamento da Internet. Outro objetivo importante é obter o comprometimento de líderes da indústria na abordagem destas questões, o que deve ampliar seu impacto, assim que mais adeptos se juntarem à iniciativa.

Objetivos

1. Aumentar a conscientização e incentivar ações, pela demonstração do compromisso crescente do grupo de apoiadores.
2. Promover a cultura de responsabilidade coletiva para a resiliência e segurança do sistema de roteamento global da Internet.
3. Demonstrar a capacidade do setor para abordar questões de resiliência e segurança do sistema de roteamento global da Internet com o espírito da responsabilidade coletiva.
4. Fornecer uma estrutura para que os provedores de acesso à Internet (ISPs) compreendam melhor e ajudem a solucionar problemas relacionados à resiliência e à segurança do sistema de roteamento global da Internet.

Escopo

Existem muitas recomendações diferentes para melhorar a segurança e resiliência do sistema de roteamento entre domínios da Internet. Algumas das orientações destas recomendações podem até parecer um pouco contraditórias, muitas vezes a decisão de adotá-las pode vir da compreensão do que é mais importante ou apropriado para uma determinada rede, considerando seu tamanho e recursos, o número de conexões externas, os clientes e usuários finais que possui, tamanho e experiência de sua equipe, e assim por diante.

As "Ações Esperadas" e "Ações Avançadas" abaixo destacam um conjunto de recomendações que são valiosas para a segurança e resiliência do sistema de roteamento global, bem como para o próprio operador de rede. Elas abordam três principais classes de problemas:

- Problemas relacionados às informações incorretas de roteamento;
- Problemas relacionados ao tráfego com endereços IP de origem falsificados (*spoofing*); e
- Problemas relacionados à coordenação e colaboração entre os operadores de redes.

As "Ações Esperadas" definem um "pacote" mínimo - um conjunto de recomendações que devem ser implementadas definitivamente pelos operadores que apoiam este documento do MANRS. Este "pacote" de recomendações não é exaustivo e a expectativa é que muitas operadoras de rede já implementem medidas e controles ainda mais rigorosos, ou planejem fazê-los no futuro. As "Ações Avançadas", explicadas mais adiante, estendem este pacote mínimo.

Estamos conscientes do fato de que qualquer Ação em particular não é uma solução abrangente para os problemas descritos. Mas cada uma delas é um pequeno passo que, se multiplicado por muitos apoiadores, pode se tornar uma melhoria significativa na resiliência do sistema global de roteamento da Internet. Portanto, a seleção de ações baseou-se em uma avaliação do equilíbrio entre pequenos custos individuais e incrementais e o potencial benefício comum.

Definições

Para articular as especificidades das "Ações Esperadas" e "Ações Avançadas", é necessário definir explicitamente vários termos, a fim de relacioná-los ao seu uso na indústria da Internet.

- **Infraestrutura –** Redes internas do operador, que devem estar acessíveis na Internet.
- **Usuário Final –** Redes no domínio administrativo e de roteamento de um operador.
- **Rede de Parceiros –** Rede externa com a qual tráfego referente à sua respectiva Infraestrutura e às Redes de Clientes é trocado.
- **Rede de Trânsito –** Rede externa para a qual o tráfego relacionado à sua Infraestrutura e às Redes de Clientes é enviado e do qual o tráfego da Internet em geral é recebido.

- **Rede do Cliente –** Rede externa para a qual um operador fornece serviços de trânsito.
- ***Single Homed* –** Link único e direto entre redes ou que conecta um Usuário Final à Infraestrutura. Representa um único caminho pelo qual o tráfego pode fluir dentro ou entre redes.
- ***Multi Homed* –** Múltiplos caminhos entre redes (até múltiplas redes), ou conexões entre um Usuário Final e a Infraestrutura; pode criar vários caminhos na Infraestrutura e na Internet pelos quais o tráfego pode fluir.

Princípios

1. A organização (ISP ou operador de rede) reconhece a natureza interdependente do sistema de roteamento global e seu próprio papel em contribuir para uma Internet segura e resiliente.
2. A organização incorpora as melhores práticas atuais relacionadas ao roteamento seguro e resiliência em seus processos de gerenciamento de rede, de acordo com as Ações estabelecidas neste documento.
3. A organização está empenhada em prevenir, detectar e mitigar os incidentes de encaminhamento por meio da colaboração e coordenação com redes de parceiros e outros ISPs, de acordo com as Ações estabelecidas neste documento.
4. A organização incentiva seus clientes e redes de parceiros a adotarem esses Princípios e Ações.

Ações Esperadas

1. Impedir a propagação de informações de roteamento incorretas.

- O operador de rede define uma política clara de roteamento e implementa um sistema que garante a correção de seus próprios anúncios e os de seus clientes para redes adjacentes com granularidade de prefixo e de AS-path.
- O operador de rede é capaz de comunicar quais anúncios estão corretos às suas redes adjacentes.
- O operador de rede avalia a exatidão dos anúncios de seus clientes, especificamente que o cliente detém legitimamente o ASN e o espaço de endereço anunciados.

2. Impedir tráfego com endereços IP de origem falsificados.

- O operador de rede implementa um sistema que permite a validação do endereço de origem para, pelo menos, redes de clientes s*ingle-homed* e s*tub*, seus próprios usuários finais e sua própria Infraestrutura. O operador de rede implementa a filtragem contra falsificação de endereço IP de origem para impedir que pacotes com endereço IP de origem incorretos entrem e saiam da rede.

3. Facilitar a comunicação operacional global e a coordenação entre os operadores de rede.

- O operador de rede mantém informações de contato atualizadas globalmente e acessíveis.

Ações Avançadas

4. Facilitar a validação de informações de roteamento em escala global.

- O operador de rede documenta publicamente sua política de roteamento, os ASNs e os prefixos que devem ser anunciados a terceiros.

Estruturação e Referências

Ação 1. Impedir a propagação de informações de roteamento incorretas.

- O operador de rede define uma política clara de roteamento e implementa um sistema que garante a correção de seus próprios anúncios e os de seus clientes para redes adjacentes com granularidade de prefixo e de AS-path.
- O operador de rede é capaz de comunicar quais anúncios estão corretos às suas redes adjacentes.
- O operador de rede avalia a exatidão dos anúncios de seus clientes, especificamente que o cliente detém legitimamente o ASN e o espaço de endereço anunciados.

Discussão: O mais importante é proteger anúncios de roteamento de entrada, particularmente de redes de clientes, por meio do uso de filtros ***explícitos*** de prefixos ou mecanismos equivalentes. Em segundo lugar, filtros de AS-path podem ser usados para exigir que a rede do cliente seja explícita sobre quais Sistemas Autônomos (ASs) estão sob a rede deste cliente. Como alternativa, os filtros de AS-path que bloqueiam anúncios de clientes de ASs com os quais o provedor tem um relacionamento de troca de tráfego podem impedir alguns tipos de vazamentos de roteamento. A filtragem de anúncios de BGP de clientes apenas por filtros de AS-path é ***insuficiente*** para impedir problemas de roteamento catastróficos em nível sistêmico.

Referências:

Recommended Internet Service Provider Security Services and Procedures, Section Network Infrastructure, http://www.rfc-editor.org/bcp/bcp46.txt

BGP operations and security, http://tools.ietf.org/html/draft-ietf-opsec-bgp-security

Border Gateway Protocol Security, NIST: Special Publication SP 800-54, http://csrc.nist.gov/publications/nistpubs/800-54/SP800-54.pdf

Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure, http://tools.ietf.org/html/rfc3871

Using RPSL in Practice, http://tools.ietf.org/html/rfc2650

Using the RIPE Database as an Internet Routing Registry, https://labs.ripe.net/Members/denis/using-the-ripe-database-as-an-internet-routing-registry

BGP Security Best Practices, FCC CSRIC III WG4 Final Report, http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG4_Report_March_%202013.pdf

Ação 2. Impedir tráfego com endereços IP de origem falsificados.

- O operador de rede implementa um sistema que permite a validação do endereço de origem para, pelo menos, redes de clientes *single-homed* e *stub*, seus próprios usuários finais e sua própria Infraestrutura. O operador de rede implementa a filtragem contra falsificação de endereço IP de origem para impedir que pacotes com endereço IP de origem incorretos entrem e saiam da rede.

Discussão: Abordagens comuns desse problema envolveram recursos de *software* como SAV (*Source-Address Validation*) em redes de *cable-modem* ou validação rigorosa de uRPF (*unicast Reverse-Path Forwarding*) em redes com roteadores. Esses métodos podem facilitar a sobrecarga de administração nos casos em que o roteamento e a topologia são relativamente menos dinâmicos. Outra abordagem poderia ser usar informações de filtro de prefixo de entrada para criar um *packet-filter*, que permitiria apenas pacotes com endereços IP de origem para os quais a rede poderia legitimamente anunciar a alcançabilidade.

Referências:

Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing, http://tools.ietf.org/html/bcp38

Ingress Filtering for Multihomed Networks, http://tools.ietf.org/html/bcp84

Securing the Edge, http://www.icann.org/committees/security/sac004.txt

RIPE Anti-Spoofing Task Force HOW-TO, http://www.ripe.net/ripe/docs/ripe-431

BGP Security Best Practices, FCC CSRIC III WG4 Final Report, http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG4_Report_March_%202013.pdf

Ação 3. Facilitar a comunicação operacional global e a coordenação entre os operadores de rede.

- O operador de rede mantém informações de contato atualizadas globalmente e acessíveis.

Discussão: Os locais comuns para manter tais informações são o PeeringDB, bancos de dados *whois* dos RIRs (Registros de Roteamento da Internet) e grandes IRRs, como RADB e RIPE. Um operador de rede deve registrar e manter informações de contato 24 horas por dia, sete dias por semana, em pelo menos um desses bancos de dados. Essas informações de contato devem incluir as informações atuais do ponto de contato do operador para o NOC do AS, todos os blocos de endereços e nomes de domínio. Os operadores são incentivados a documentar suas políticas de roteamento de rede em um IRR. Informações adicionais também são bem-vindas, como, por exemplo, uma URL de visualização no campo apropriado em seu registro do PeeringDB.

Referências:

Using RPSL in Practice, http://tools.ietf.org/html/rfc2650

Peering DB, https://www.peeringdb.com

RADB, http://www.radb.net/

Ação 4. Facilitar a validação de informações de roteamento em escala global.

- O operador de rede documenta publicamente sua política de roteamento, os ASNs e os prefixos que devem ser anunciados a terceiros.

Discussão: Para facilitar a validação de informações de roteamento por outras redes em escala global, informações sobre políticas de roteamento, ASNs e prefixos que devem ser anunciados às redes externas são necessárias.

Uma das formas de disponibilizar publicamente a política é documentá-las usando o RPSL em um dos Registros de Roteamento da Internet (IRRs) espelhados pelo RADB (por exemplo, RIPE, ARIN, RADB etc.). Nesse caso, os operadores devem registrar e manter no mínimo um (ou mais) objetos IRR contendo uma lista de ASNs destinados a serem anunciados a terceiros, que podem ser usados por ferramentas automáticas para gerar filtros de prefixo. Os operadores também devem manter suas informações na IRR e garantir que estejam atualizadas.

Outro meio, mais seguro, para facilitar a validação em escala global é por meio do sistema RPKI. Operadores podem obter certificados RPKI para seus próprios prefixos dos RIRs que alocaram esses prefixos para eles, e publicar e manter os ROAs (*Routing Origin Authorizations*) correspondentes aos prefixos que anunciam.

Operadores devem incentivar os operadores da sua Rede de Clientes a também fazê-lo. Isso permitirá que outras redes validem anúncios na escala global.

Referências:

Using RPSL in Practice, http://tools.ietf.org/html/rfc2650

Using the RIPE Database as an Internet Routing Registry, https://labs.ripe.net/Members/denis/using-the-ripe-database-as-an-internet-routing-registry

Origin Validation Operation Based on the Resource Public Key Infrastructure (RPKI), http://www.rfc-editor.org/bcp/bcp185.txt