Quarta-feira, 1 de agosto de 2018; 14:30-16:00 h.

Sessão 7

Desafios na Gestão de Identificadores da Internet

Primeira seção

Quatro temas foram desenvolvidos, cada um por um especialista, que, em 7 minutos, levantou a introdução de cada assunto, além de seus desafios e problemas na seguinte ordem: Bloqueios para sites/redes, por Raquel Gatto (ISOC); Preparação contra desastres, por Lito Ibarra (SVNET); Privacidade sob a abordagem do GDPR e seu impacto no DNS, por Rodrigo de la Parra (ICANN); e Segurança de Roteamento, por Guillermo Cicileo (LACNIC).

Bloqueios a sites/redes: Raquel Gatto, ISOC

- O conceito de bloqueio na Internet é uma interrupção total ou parcial das comunicações eletrônicas; o mesmo pode ocorrer em países, grupos de pessoas ou de serviços.
- A Internet Society apresentou um estudo que abrange as principais técnicas para realizar bloqueios: bloqueio baseado no protocolo e no IP, bloqueio baseado na inspeção profunda de pacotes (DPI), bloqueio baseado nas URL, bloqueio baseado na plataforma e bloqueio baseado no DNS.
- Os bloqueios nem sempre são eficientes, pois nem sempre cumprem o objetivo de interromper os serviços e geram efeitos colaterais prejudiciais para o ecossistema, tanto em termos de direitos humanos quanto em questões econômicas e em aspectos técnicos para as redes.
- Um caso emblemático foi a tentativa de bloquear o Whatsapp, que não funcionou de forma eficiente e teve repercussões nos países da região.

Preparação contra desastres: Lito Ibarra (SVNET)

- Durante o LACIGF, vários aspectos da camada de usuários foram discutidos, incluindo os esforços para conectar mais pessoas à Internet.
- No entanto, na base de tudo, a infraestrutura das redes continua presente, mesmo que esteja sujeita a desastres. De tal forma que a promoção de aplicativos maiores e serviços baseados na Internet tornam os usuários mais dependentes do acesso à Internet.
- Uma das questões relacionadas aos desastres naturais é a proteção da infraestrutura crítica que nos permite permanecer conectados. Infelizmente, nem todos os desastres naturais podem ser previstos.
- Os sistemas que estão em risco são os servidores que resolvem os nomes de domínio, os pontos de troca de tráfego, os bancos de dados, os provedores

de conectividade local e internacional, bem como a infraestrutura diversa (cabos, fibras, links, roteadores, switches ...)
- Embora existam várias medidas de mitigação, algumas delas não são adotadas até que ocorra algum desastre natural.

Privacidade sob a abordagem do GDPR e seu impacto no DNS. Rodrigo de la Parra (ICANN)

- As medidas de privacidade e proteção de dados da União Europeia fazem parte das discussões da comunidade da ICANN há algum tempo. Nesta ocasião, a questão é tratada no contexto de suas implicâncias para a governança da Internet.
- O GDPR (Regulamento Geral de Proteção de Dados) foi emitido pela União Europeia e entrou em vigor em 25 de maio de 2018; é aplicável a empresas que processam dados pessoais de indivíduos residentes na União Europeia. O descumprimento implica multas de grandes quantias.
- O GDPR afeta ao Sistema de Nomes de Domínio em pelo menos duas áreas:
    - Em relação às partes contratadas, conforme coletam, exibem e processam dados pessoais. Entre esses atores se encontram os registros e os registradores.
    - Internamente, a ICANN coleta alguns dados pessoais e os processa para serviços internos.
- Uma das soluções propostas pela comunidade da ICANN foi a Especificação Temporária, que fornece um modelo provisório unificado, para que as disposições contidas no GDPR sejam cumpridas e, ao mesmo tempo, o funcionamento dos serviços de registro, como o WHOIS, seja garantido.
    - Além disso, a comunidade de múltiplas partes interessadas da ICANN terá a tarefa de definir uma política que aborde as mudanças geradas pela entrada em vigor do GDPR.

Segurança de roteamento: Guillermo Cicileo (LACNIC)

- O roteamento na Internet é um dos pilares para seu funcionamento, com base no BGP: No entanto, como foram projetados há algum tempo, existem várias considerações de segurança que não foram levadas em consideração.
- Houve várias propostas para resolver as preocupações relacionadas à segurança de roteamento, como o RPKI. No entanto, a adoção de tais medidas ainda é baixa, pelo que uma das intenções é promover sua adoção entre os atores relevantes.
- Também é possível aderir ao programa MANRS, a fim de aumentar as medidas de segurança entre os provedores de acesso à Internet.

Segunda seção:

Os problemas e desafios de cada questão foram compartilhados com os participantes da sessão nas telas do salão. Posteriormente, os participantes foram divididos em quatro grupos (cada um com um moderador e um relator) para manter 30 minutos de discussão construtiva e aberta sobre os problemas, desafios e melhores práticas de cada tópico. Os relatores para cada tema foram: Alexandra Dans (ICANN) para o tema "Bloqueios a sites/redes"; Shernon Osepa (ISOC) para o tema "Preparação contra desastres"; Gabriela Ramírez (.AR) para o tema "Privacidade sob a abordagem do GDPR e seu impacto no DNS"; e Carolina Caeiro (LACNIC) para o tema "Segurança de Roteamento".

As perguntas para desencadear a discussão foram as seguintes:

Bloqueios a sites/redes:

- Quais usuários e serviços da Internet são afetados pelas técnicas de bloqueio da Internet?
- Quais são os efeitos mais comuns nos direitos humanos, na economia e na estabilidade da rede?
- Quais são os papéis dos diferentes atores no processo de bloqueios da Internet: governos, usuários, comunidade técnica, setor privado?
- Quais são os processos e suas características em bloqueios?

Preparação contra desastres:

- Quais medidas de mitigação podem ser tomadas?
- Quem deve estar interessado na prevenção de danos?
- Qual é o papel de cada parte interessada (sociedade civil, governo, iniciativa privada, academia, comunidade técnica)?
- Quais componentes do sistema de conectividade devem ser protegidos?
- De onde devem vir os recursos para desenvolver medidas de prevenção ou mitigação?
- É um trabalho a nível nacional ou internacional?
- Esta questão deve ser incluída na Governança da Internet?

Privacidade sob a abordagem do GDPR:

- Em sua opinião, como deve ser alcançado um equilíbrio entre os objetivos de privacidade/proteção de dados pessoais e os objetivos de segurança e da estabilidade operacional?
- Quais foram as lições aprendidas em relação ao impacto de um regulamento regional sobre aspectos globais da Internet?
- O modelo de múltiplas partes interessadas e o desafio da reação eficiente perante eventos externos.

Segurança de roteamento:

- Quais são os problemas que podem afetar o usuário final se o sistema de roteamento falhar?
- Que medidas existem para mitigar esses problemas?
- Como fazer para que os ISP adotem essas medidas?
    - Validação: trabalho forte com os NOG, IXP, etc.
    - Adoção do RPKI:
        - Capacitação dos operadores.
        - Maior difusão no ecossistema da Internet.
        - Adesão ao MNRS (reputação dos ISP).
    - Adoção e monitoramento de padrões pelos operadores.

Terceira seção:

O público foi reunido novamente, para que os relatores compartilhassem os resultados dos debates em cada grupo.

Bloqueios a sites/redes: Alexandra Dans, ICANN

- Vários motivos foram apontados para impulsionar bloqueios, incluindo exemplos concretos:
    - No Uruguai, tentou-se executar um bloqueio por motivos de jogo. O jogo é legal no país, mas é regulamentado.
    - Foram apontados vários casos na Venezuela, bem como algumas soluções para tentar ignorar os bloqueios, incluindo usos de DNS alternativos.
- As perspectivas éticas do bloqueio também foram discutidas, destacando que existem motivos legítimos, como a luta contra a pornografia infantil.
- Algumas questões surgiram, incluindo aspectos legítimos para ordenar os bloqueios, particularmente no que diz respeito à legitimidade das autoridades competentes para ordená-los. Caso tal legitimação não exista, os bloqueios podem ser legais, mas não seriam éticos.

Preparação contra desastres: Shernon Osepa, ISOC

- Uma das experiências compartilhadas foi a do México, após o terremoto de setembro de 2017: muitos usuários tentaram fazer uso de serviços baseados na Internet, excedendo a capacidade da infraestrutura. Algumas opiniões sugeriram a divulgação de conselhos sobre o uso da Internet após desastres.
- No caso da Guatemala, é suscetível a desastres causados por vulcões, de modo que a prevenção e o monitoramento assumem especial relevância.
- Para o Haiti, a coordenação local entre os operadores e o governo tornou-se especialmente relevante em casos de desastre.
- Em relação à prevenção de danos, foi mencionada a importância de propor soluções holísticas, a fim de incorporar as preocupações e melhores práticas de todas as partes interessadas.
- Além disso, os participantes concordaram que a prevenção e a recuperação em casos de desastres é uma questão importante para a comunidade de governança da Internet.

Privacidade sob a abordagem de GDPR e seu impacto no DNS. Gabriela Ramirez, .AR

- Em relação ao equilíbrio entre privacidade e segurança, os participantes apontaram que não há antagonismo entre tais características, de modo que as informações que sejam coletadas devem ser relevantes, a fim de evitar abusos em tais casos.
- Também foram mencionadas as diferenças entre os ccTLDs e os gTLDs, que têm um relacionamento diferente com a ICANN, de modo que as obrigações de cada ator são diferentes.
- As legislações locais sobre proteção de dados foram identificadas como um elemento importante na discussão.
- O GDPR foi identificado como uma oportunidade para a comunidade rever seus mecanismos de coleta, tratamento e proteção de dados pessoais, a fim de salvaguardar os interesses dos usuários finais.

Segurança de roteamento: Carolina Caeiro, LACNIC

- Os participantes colocaram vários exemplos que ocorreram na comunidade em relação aos ataques de roteamento.
- Além disso, foi apontado que alguns ataques de roteamento não são percebidos pelos usuários finais.

- Com relação às medidas de prevenção e reforço de segurança no roteamento, foram colocadas algumas como o RPKI e o BGPsec, incluindo aspectos concretos como a necessidade de que as conexões de BGP incorporem senhas para cada roteador.
- A iniciativa de MANRS da Internet Society foi apontada como uma das medidas de prevenção para fortalecer a segurança do roteamento.
- Ela também destacou a necessidade de cooperação entre os operadores, não apenas em nível nacional, mas também entre países.
- A capacitação foi identificada como um elemento-chave, não apenas para os operadores, mas para vários atores da comunidade da Internet.

Relator:

Israel Rosas, Outreach Manager LAC, Internet Society