ICANN|55
MARRAKECH
5 – 10 MARCH 2016

RELATÓRIO DNS.PT

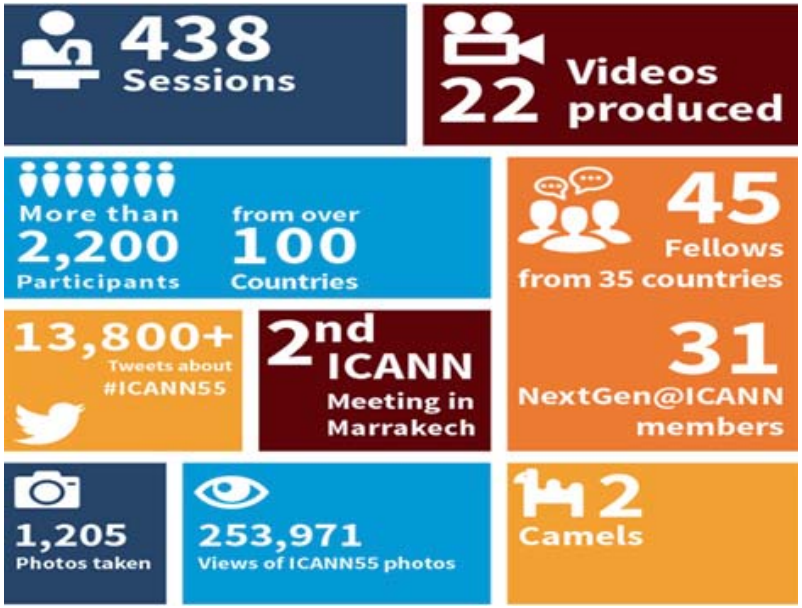
ÍNDICE

A 55.ª edição da ICANN ficou marcada com dois acontecimentos especiais: a conclusão e aprovação do Plano de transição das funções da IANA a submeter à NTIA e a despedida de Fadi Chehadé que deixa a presidência do ICANN que passará, já no mês de maio, para o sueco Göran Marby.

"*This plan is a testament to the hard work of the global Internet community and the strenght of the mulistakeholder model*", Dr. Sephen Crocker, chair/ICANN

Esta edição decorreu na cidade de Marraquexe, em Marrocos, entre os dias 5 e 10 de março de 2016 sob o alto patrocínio do rei Mohammed VI. O ccTLD deste país - .ma – é registável em www.internic.ma e conta hoje com perto de 60 000 domínios.

ICANN 55 em números:



ICANN pelo mundo:

Como dito, o encerramento da 55.º edição da ICANN ficou marcado com o encaminhamento ao governo dos EUA/NTIA (National Telecommunications & Information Administration) do plano de suporte à transição das funções técnicas da IANA (Internet Assigned Numbers Authority), amplamente críticas para o funcionamento da Internet. Este plano encerra ainda um conjunto de propostas no sentido de alterar o processo de prestação de contas da ICANN que passará a assumir-se como uma organização inteiramente independente de vínculos governamentais.

Em março de 2014, a NTIA anunciou a sua intenção de proceder à transição das funções-chave da Internet para a comunidade Internet. A NTIA solicitou em concreto à ICANN que "(...) *convocasse um processo multistakeholder para desenvolver um plano para a transição do papel de gestão do governo EUA*". Para além dos grupos de trabalho (ICG e CCWG - Accountability) que ao longo destes últimos dois anos se debruçaram no desenho do Plano final, tratou-se de um processo altamente participado por representantes do governo, comunidade técnica, especialistas oriundos de várias áreas, academia e sociedade civil em geral. Foram registadas nestes âmbito 600 reuniões e chamadas, mais de 32.000 trocas de e-mails e mais de 800 horas de carga horária.

"*A comunidade Internet demonstrou ter uma dedicação extraordinária para a transição da supervisão porque sabemos quão importante é finalizar esse processo*", disse Alissa Cooper,

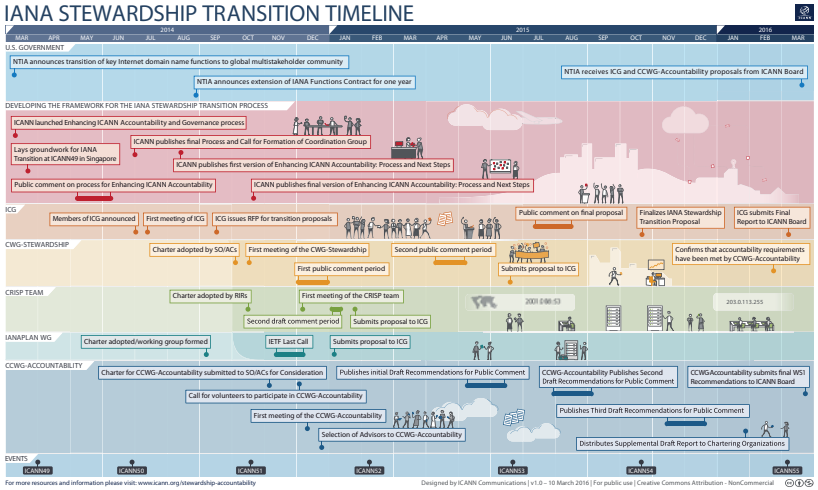
presidente do Grupo de Coordenação da Transição da Supervisão da IANA (ICG), que coordenou a elaboração da proposta da transição.

"Este plano reflete o mais amplo apoio desta comunidade tão diversa e estou certo de que ele vai satisfazer os critérios da NTIA," disse Thomas Rickert, um dos copresidentes do CCWG-Prestação de Contas.

Nas palavras de Steve Crocker: "*O plano foi enviado agora ao governo dos EUA para sua revisão e, se ele cumprir os critérios necessários, teremos alcançado um momento histórico na história da Internet*".

Cumpre agora ao governo dos EUA analisar o Pacote submetido pela ICANN certificando-se que cumpre os princípios e critérios definidos inicialmente pela NTIA. Se o plano for aprovado, a respetiva implementação deverá ficar finalizada antes do termo do contrato entre a NTIA e a ICANN, em setembro de 2016.

Assim decorreu o processo:



https://www.icann.org/sites/default/files/assets/iana-stewardship-timeline-10mar16-en.pdf

Survey do CENTR: dezembro de 2015/24 respostas

O CENTR realizou no passado mês de dezembro um inquérito aos seus associados, sobre o tratamento de algumas questões de natureza jurídica no âmbito do processo de registo e manutenção de domínios. Responderam 24 registries.

No que respeita em particular aos conteúdos associados aos domínios, 70% dos registries afirmaram nunca lhes ter sido solicitada a remoção de um domínio pelo facto de alojar conteúdos ilegais. No entanto, 46% afirma já ter recebido uma ordem de um tribunal no sentido de restringir o acesso a determinado conteúdo. Na mesma percentagem estão incluídos os registries que já foram parte numa ação em Tribunal relacionada com conteúdos, sendo que destes, 82% dos casos diziam respeito a violações em matéria de propriedade intelectual. Por fim, 61% dos registries tem o entendimento claro de não se incluir no conceito de intermediário na aceção da diretiva do comércio eletrónico.

ICANN 55 - Sessões Técnicas

A comunidade técnica internacional reuniu-se uma vez mais em Marraquexe, para participar nas sessões do ICANN, em torno da apresentação e discussão de projetos e questões do foro tecnológico, relacionados com a evolução e segurança da Internet.

Destacamos as sessões de *Tech Day* e do habitual *Workshop DNSSEC*.

ICANN | 55 • TECH DAY

A sessão Tech Day sucedeu à cerimónia de abertura da 55ª reunião do ICANN, e foi moderada por Eberhard Lisse, Chair do ccNSO Technical Working Group. A sessão iniciou com um breve resumo da agenda de trabalhos, os quais passamos a resumir.

KNOT Resolver, A flexible DNSSEC-validating Resolver

A primeira apresentação desta sessão ficou a cargo de Ondřej Surý do .CZ, que nos falou do *software KNOT Resolver*[1]. Trata-se de um projeto muito recente, que está a ser desenvolvido pelo CZ.NIC Labs, o departamento de pesquisa e desenvolvimento do CZ.NIC, um *Registry* que tem dado um contributo tecnológico à comunidade Internet, com vários projetos[2] de *software* e inclusive de *hardware*.

O *software KNOT Resolver,* é uma aplicação *open source* (GPLv3+), para servidores de nomes recursivos, com suporte total para DNSSEC, incluindo os mais recentes desenvolvimentos como algoritmos de criptografia das curvas elípticas ECDSA (RFC 6650), a gestão automática da *Trust Anchor* (RFC 5011), e *Trust Anchors* negativas (RFC 7646). No campo do IPv6, tem suporte para "Happy Eyeballs" (RFC 6555).

É uma aplicação modular muito versátil, desenvolvida em C e LuaJIT e configurável por scripts, cujo objetivo é evoluir a componente de rede responsável pela resolução de nomes DNS

dentro das organizações, com especial destaque para os operadores de serviços Internet (ISP's) que gerem uma ou mais redes de clientes.

Ondřej Surý enquadrou o uso desta solução em diferentes cenários, desde grandes sistemas recursivos complexos, até projetos de investigação e o uso por utilizadores fans destas tecnologias 'Geeks'.

De notar que .CZ reutilizou o nome KNOT neste projeto, não obstante de já ter desenvolvido anteriormente, o *software* KNOT DNS exclusivamente para o serviço DNS autoritativo.

[1] https://www.knot-resolver.cz/
[2] https://labs.nic.cz/en/projects.html

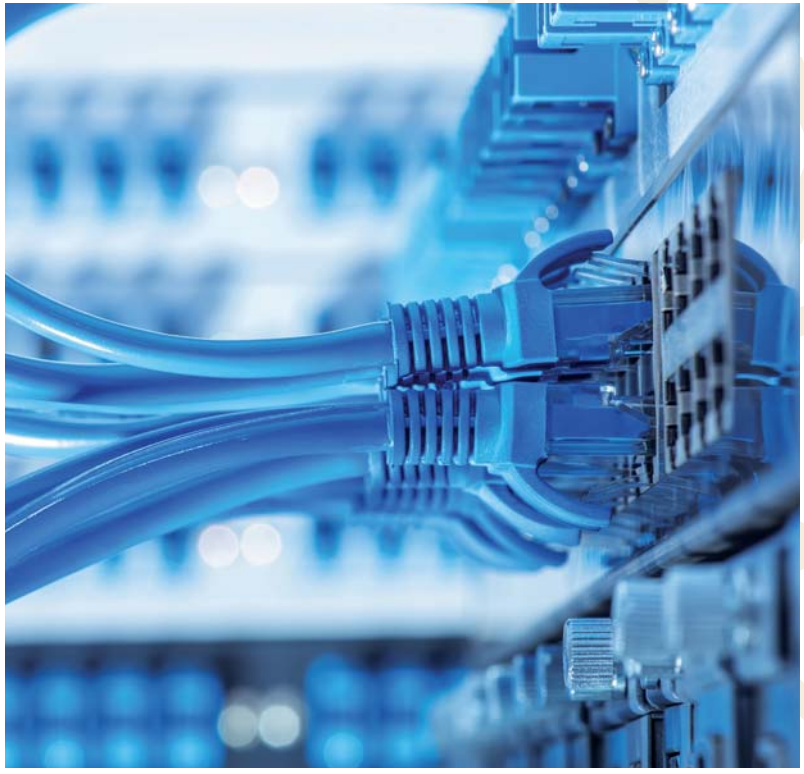
EAI (IDN E-Mail) - From Standard To Commercialization

Marvin Woo apresentou a integração dos serviços de email da Coremail[3] com as normas de *Email Address Internationalization (EAI)*, ou seja, a utilização de UTF-8 no serviço de email, para representar carateres do padrão Unicode (chineses e outros), nas componentes local, anterior à "@", e de domínio, que compõem um endereço de email. Coremail é uma plataforma de email desenvolvida a partir de 1999 e conta atualmente com 700 milhões de utilizadores na China, entre empresas, instituições governamentais, universidades e um vasto leque de organizações.

A solução apresentada incorpora desde 2012, os protocolos e as normas tecnológicas internacionais para integração do UTF-8 no serviço de email, nomeadamente o envio por SMTP com UTF-8 (RFC 6531), a utilização de UTF-8 nas extensões MIME (Multipurpose Internet Mail Extensions) (RFC 6532), o suporte de UTF-8 para IMAP (RFC 6855) e para POP3 (RFC 6856). Tem mecanismos de fallback, ou seja quando não consegue transmitir uma mensagem no formato EAI, transmite no formato normal com carateres do ASCII também conhecido por Latim.

Nos últimos anos, a organização tem feito um conjunto de iniciativas para promover a comercialização da solução, nomeadamente o lançamento de aplicações para as plataformas Android, iOS, Windows, Flash Mail e Lunkr, a adaptação para as linguagens Tailandesa e Hindi, e a atualização da plataforma SaaS da Coremail.

A estratégia dos próximos anos passará por popularizar a utilização de email com EAI na China e noutros países com as mesmas questões linguísticas face a tecnologia existente, e implementar aplicações com EAI em círculos fechados, como o exército e o governo.



[3] http://www.coremail.cn/

EBERO Exercise

Francisco Arias, Diretor dos serviços técnicos da ICANN e Simon McCalla da Nominet, apresentaram os resultados de um simulacro do programa *Emergency Back-End Registry Operator* (EBERO[4]). O programa EBERO faz parte do programa dos novos gTLDs, o seu objetivo é garantir uma das missões básicas da ICANN, preservar a segurança e a estabilidade operacionais da Internet.

Em termos concretos, o programa EBERO legitima a ICANN, a tomar a iniciativa de transferir a operação dum gTLD para um operador EBERO, numa situação de emergência. É considerada uma situação de emergência quando um Registry não consegue manter determinadas funções críticas de registo de domínios. Um operador EBERO é uma entidade previamente contratada pelo ICANN, responsável por um conjunto de funções preestabelecidas, que visam garantir a operacionalidade de gTLD's numa situação de emergência. A ICANN é responsável por declarar um evento EBERO e coordenar todas as atividades de resposta a emergências.

O exercício de simulação foi feito com o gTLD .doosan[5], um domínio de topo autêntico. A 3 de setembro de 2015, o Registry deste domínio de topo, solicitou a cessação do contrato com a ICANN a partir do dia 1 de março de 2016. Tratava-se de um domínio de topo que não tinha qualquer domínio registado de *Registrants*. O Registry de .doosan, e o operador EBERO selecionado, a Nominet, aceitaram a realização do exercício de simulacro, proposto pelo ICANN. Estavam assim reunidas as condições para testar o programa EBERO.

A simulação do evento EBERO relatada nesta sessão teve início no dia 26 de janeiro às 12:00 UTC. Os resultados foram os seguintes:

- Indisponibilidade do serviço DNS (simulado e sem contar com efeitos de caching): 12 hours, 22 minutes
- Indisponibilidade da informação de registo - Whois, (simulado e sem contar com efeitos de caching): 2 days, 5 hours, 5 minutes
- Os serviços partilhados de registo - EPP, restaurados em 1 dia, 23 horas e 3 minutos depois de detetado o incidente (4 horas após o início do exercício)
- A função de Data Escrow (fim do exercício), restaurada ao fim de 5 dias, 21 horas, 53 minutos depois de detetado o incidente
- Durante o exercício, foram identificadas 44 oportunidades de melhoria/correção do projeto

Francisco Arias considerou que a reposição do serviço DNS, 12 horas após detetado o incidente, constitui um sucesso impressionante do programa EBERO. Para Simon McCalla foi um teste esmagadoramente bem-sucedido, de um processo que foi construído de forma colaborativa entre os operadores EBERO e a ICANN e irá continuar a evoluir dessa forma, à medida que o serviço DNS vai também ele evoluindo. Por último, uma nota de que este programa é um processo especificamente desenhado em torno da transição de um gTLD para um operador EBERO, e não como um processo de resiliência.

[4] https://www.icann.org/resources/pages/ebero-2013-04-02-en
[5] https://www.icann.org/resources/agreement/doosan-2014-04-03-en

DDoS Attack on .TR

Atilla Özgit do .TR o ccTLD da Turquia, apresentou os dados do incidente de segurança informática de que foram alvo no final de 2015.

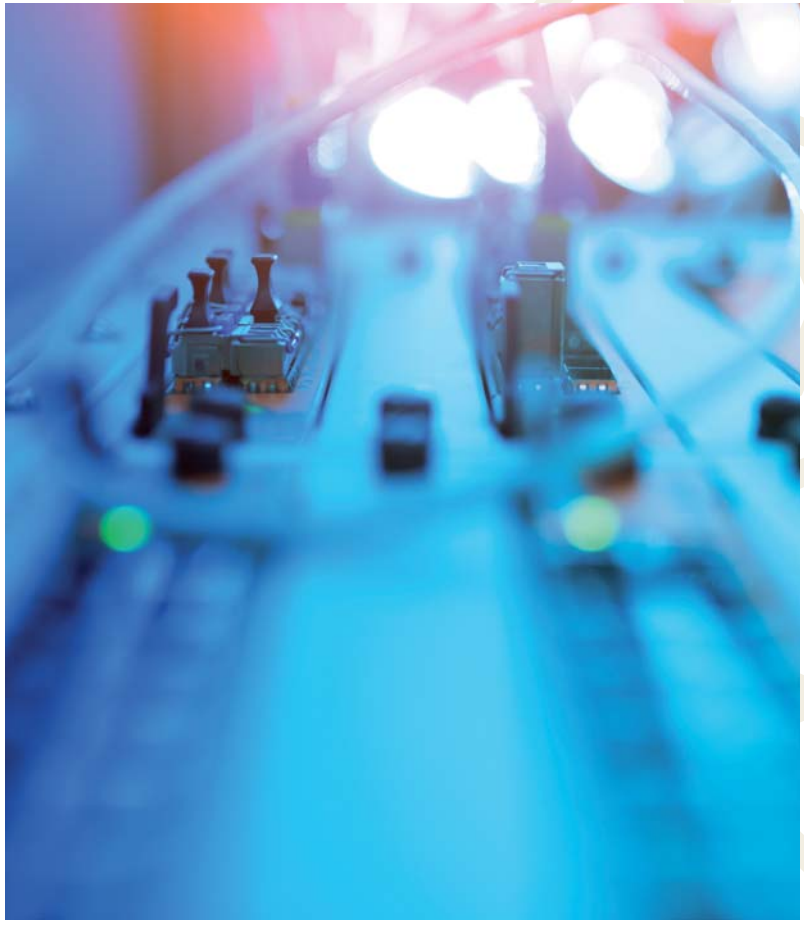
Tratou-se de um ataque distribuído de negação de serviço (DDOS), onde foram utilizadas técnicas de amplificação/reflexão, que permitem um aumento da quantidade de tráfego DNS gerado, encobrindo simultaneamente a fonte deste ataque.

Destacamos as seguintes características do incidente:

- Começou a 14 de dezembro de 2015, e prevaleceu aproximadamente nas três semanas seguintes;
- O ataque ocorria em turnos, sendo que o principal turno ocorria em horas de expediente, entre as 9:00 e as 17:00, com um volume de tráfego DNS perto das 185.000 qps (consultas por segundo), por servidor;
- Nos restantes turnos, o volume de tráfego reduzia e os sistemas que estavam a enviar o trafego DNS mudavam;
- Em uma das três ligações do .TR à Internet, foi detetado o uso de 220 Gbps de largura de banda;
- A componente de ataque adaptava-se rapidamente as medidas contenção adotadas pelo .TR durante o incidente.

Após o incidente, o .TR reforçou a resiliência da sua infraestrutura DNS, através do aumento da superfície de ataque, e da análise de tráfego para a implementação de filtros. Também reduziu a frequência de publicação de atualizações da zona .TR, e iniciou um processo manual de inspeção das delegações efetuadas em .TR.

Nas conclusões, é realçada a importância de ter bons canais de comunicação com todos os intervenientes, nomeadamente a IANA, a equipa interna do Registry, os operadores que fornecem conectividade ao Registry, e entidades nacionais de Cibersegurança.



TLD-OPS Update

Cristian Hesselman, o chair do grupo de trabalho *Secure Email Communication for ccTLD Incident Response (SECIR)* do ccNSO, fez uma atualização do projeto TLD-OPS.

Este projeto agrega um repositório de contactos – nome, email, endereço e número de telefone – de todos os ccTLD's, com o objetivo de tornar mais fácil e imediato os contactos interpares, sobretudo na sequência de problemas e ataques de segurança. A participação está aberta a qualquer ccTLD, não é necessário ser membro do ccNSO.

Este grupo de trabalho é supervisionado pelo TLD-OPS Standing Committee, composto por representantes de ccTLDs, SSAC, IANA, e a equipa de segurança da ICANN.

Atualmente, as estatísticas de adesão de ccTLDs a esta iniciativa são as seguintes:

All	Members	%	Missing	%	Total
Total	***173***	60%	***117***	40%	***290***

ASCII	Members	%	Missing	%	Total
Total	***145***	***59%***	***99***	***41%***	***244***
AF	22	45%	27	55%	49
AP	42	51%	41	49%	83
EU	62	95%	3	5%	65
LAC	16	38%	26	62%	42
NA	3	60%	2	40%	5

IDN	Members	%	Missing	%	Total
Total	***28***	61%	***18***	39%	***46***

Last update: Mar 5, 2016

Desde da última reunião do ICANN em Dublin, foram adicionados os seguintes ccTLD's: Egito, Argélia, Barbados, Gibraltar, Moldávia e a Bósnia e Herzegovina. A maior dificuldade continua a ser a inclusão de países das regiões de Africa, Asia e do Pacífico, e América Latina.

O projeto tem agora pela frente dois desafios, o primeiro é promover a partilha de informação de incidentes de segurança entre membros da lista, o segundo desafio é a inclusão dos novos gTLDs. Esta hipótese foi apresentada na reunião do ccNSO e foi aprovada pelos presentes.

Q&D DNSSEC Monitoring

Jaap Akkerhuis da NLnet Labs[6], apresentou uma metodologia simples para testar DNSSEC em todos os domínios de topo delegados na Internet, baseada no software Unbound, desenvolvido pela própria NLnet Labs.

O apresentador mantém esta solução ativa desde janeiro de 2012, e as situações que encontra com mais frequência são as seguintes:

- Assinaturas DNSSEC expiradas;
- Algoritmos de encriptação que não coincidem;
- Assinaturas DNSSEC em falta;
- Os servidores de nomes falham em responder: Servfail

A solução tem algumas limitações, nomeadamente quando acontece problemas de rede o que resulta em resultados falsos negativos.

Thoughts on F-Root Futures

Vicky Risk do *Internet Systems Consortium* (ISC) apresentou a posição estratégica do ISC para o serviço de *Root Server*[7] do servidor "F-Root".

Um *Root Server* é um servidor DNS que serve a zona raiz de topo do serviço DNS, onde estão delegados todos os domínios de topo, tal como os gTLDs e os ccTLDs, nomeadamente o domínio ".PT". Inicialmente existiram 13 *Root Servers*, nomeados de "*a.root-servers.net*" a "*m.root-servers.net*", atualmente graças à tecnologia de *Anycast*, o número de réplicas de *Root Servers* é amplamente superior, existem 572 localizações com o serviço de *Root-Server* em todo o mundo. Tradicionalmente uma instância/réplica de *Root Server*, é composta por uma infraestrutura robusta com um grau de complexidade elevado que requer conhecimento especializado para efetuar a sua gestão.

Atualmente o servidor "F-Root" é um dos 13 *Root Servers* iniciais, é gerido pelo ISC e tem um total de 58 réplicas em 50 países.

O ISC entende que a realidade atual, induz uma alteração no paradigma do serviço de *Root Server*, para explicar melhor esta alteração o ISC apoiou-se nos exemplos da natureza com a seguinte afirmação "como num exame, o que interessa é quantos sobrevivem, e não quantos são devorados por predadores".

O ISC propõe uma solução de servidor *Root Server* conhecida por "*F-Single*". É uma solução mais simples, com custos reduzidos, que deverá ser implementada sobretudo em localizações com menos cobertura de resolução DNS como Africa.

6 http://www.nlnetlabs.nl/

7 https://www.iana.org/domains/root/servers

A Geek's Guide to Universal Acceptance

An update to TechDay

Don Hallander da ICANN apresentou uma atualização da iniciativa "*Universal Acceptance*". O conceito desta iniciativa, é que todos os nomes de domínios e endereços de email devem ser aceites, armazenados, processados e exibidos de uma forma consistente e efetiva.

Muitas aplicações assume que os nomes de domínios e os endereços de email associados, apenas existem no formato ASCII, e que os domínios de topo estão restritos a um conjunto bem definido de nomes com dois ou três carateres. Mas com a introdução de domínios de topo de *ccTLDs com Internationalized Domain Names (IDNs)* em 2010, e mais recentemente a partir de 2013, com a introdução de novos gTLDs, esse cenário deixou de ser uma realidade.

A iniciativa Universal Acceptance (UA) foi formalmente criada em fevereiro de 2015, através da criação do grupo de trabalho Universal Acceptance Steering Group (UASG) , que visa promover a aceitação universal de todos os domínios e endereços de email. O UASG é um grupo suportado pela ICANN, e do qual participam ativamente organizações, como a Afilias, a Apple, o .Asia, ccTLDs (.rs, .th, e outros), Donuts, GoDaddy, Google, Microsoft, The DNA, Verisign e muitos outros.

Segundo Don Hallander, esta iniciativa tem forçosamente que passar pelos utilizadores altamente adeptos de tecnologia, mais conhecidos por "geek's". Um pouco à semelhança do problema do bug do ano 2000, este problema é global com uma solução distribuída, é um problema maioritariamente de software e não tanto de hardware, não é um problema difícil mas é desafiante e requer grande empenho, e por último ainda é necessário quebrar algumas barreiras nomeadamente as normas de Email Address Internationalization (EAI), e outras situações como o alfabeto árabe, e o hebraico onde a escrita se efetua da direita para a esquerda.

Neste momento o grupo de trabalho UASG[8] está a desenvolver documentação e a abordagem ao problema. Posteriormente irá criar uma lista de ferramentas adaptadas a UA (UA Ready), lançar campanhas de sensibilização, e agilizar a implementação das normas EAI.

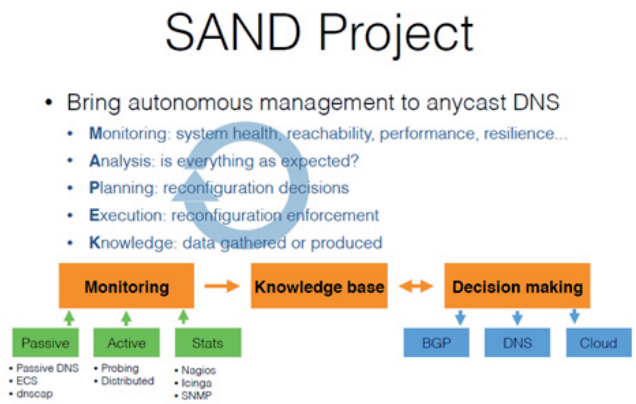
[8] https://community.icann.org/pages/viewpage.action?pageId=47255444

SAND Project - Self-managing Anycast Networks for the DNS

Ricardo Schmidt da Universidade de Twente na Holanda, falou-nos do projeto académico de investigação Self-managing Anycast Networks for DNS (SAND). Este projeto iniciou em novembro de 2014, e tem a participação da Universidade de Twente, o SIDN o ccTLD do .NL, e a NLnet Labs uma fundação sem fins lucrativas que desenvolve software open source para a Internet.

Este projeto foca-se no desenvolvimento de mecanismos de gestão autónoma do serviço DNS, nomeadamente em nuvens de Anycast. Estes mecanismos deverão ser capazes de reagir e atual em cenários de alterações de conectividade na Internet, volume de tráfego DNS e outros fatores determinantes para a segurança e o desempenho do serviço DNS.

A estrutura do projeto é identificada na seguinte imagem.



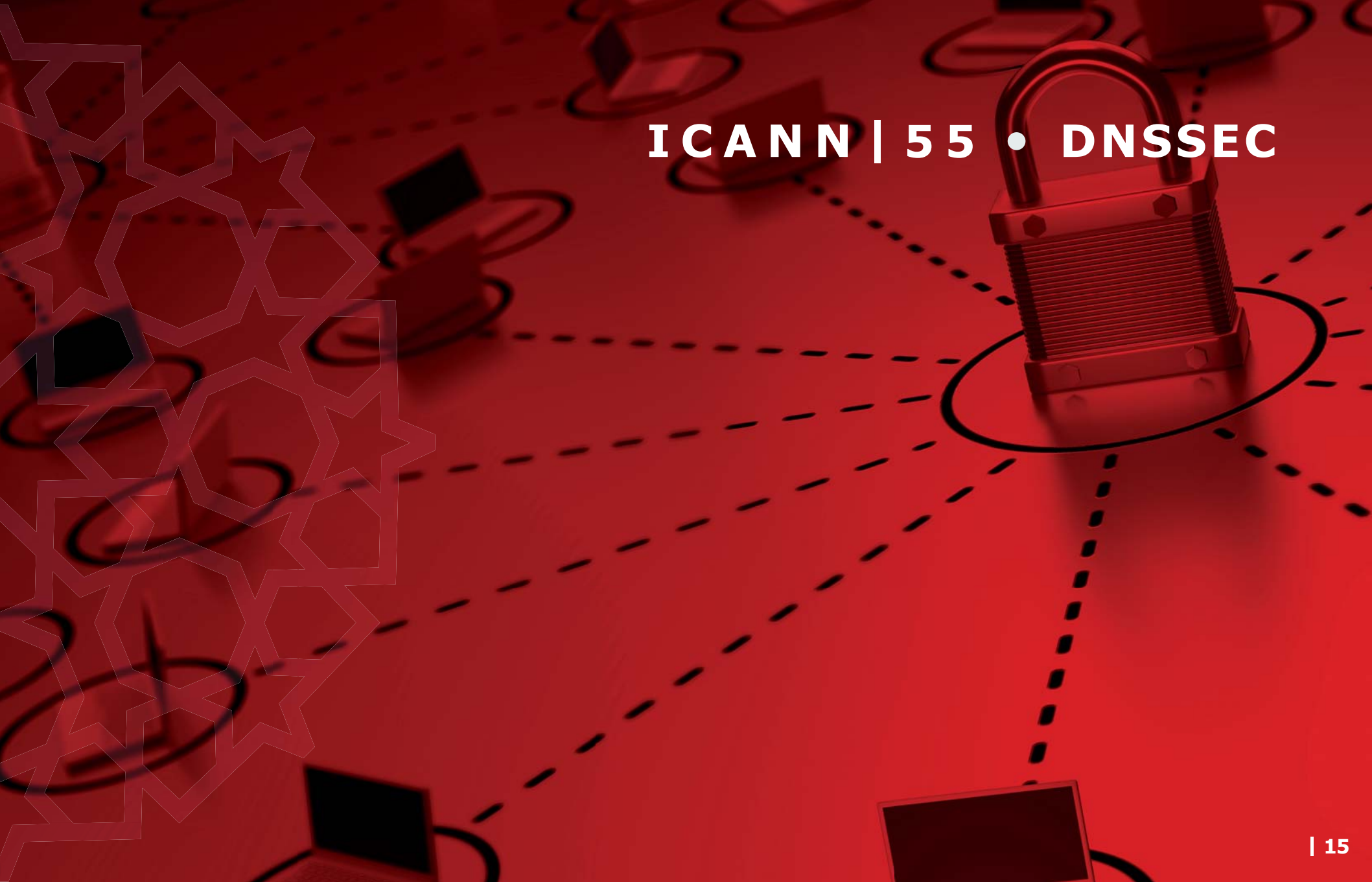
O trabalho já efetuado centra-se sobretudo em monitorização, com recurso ao projeto Ripe Atlas. Está a ser implementada uma nuvem global de Anycast para servir de plataforma de investigação e testes.

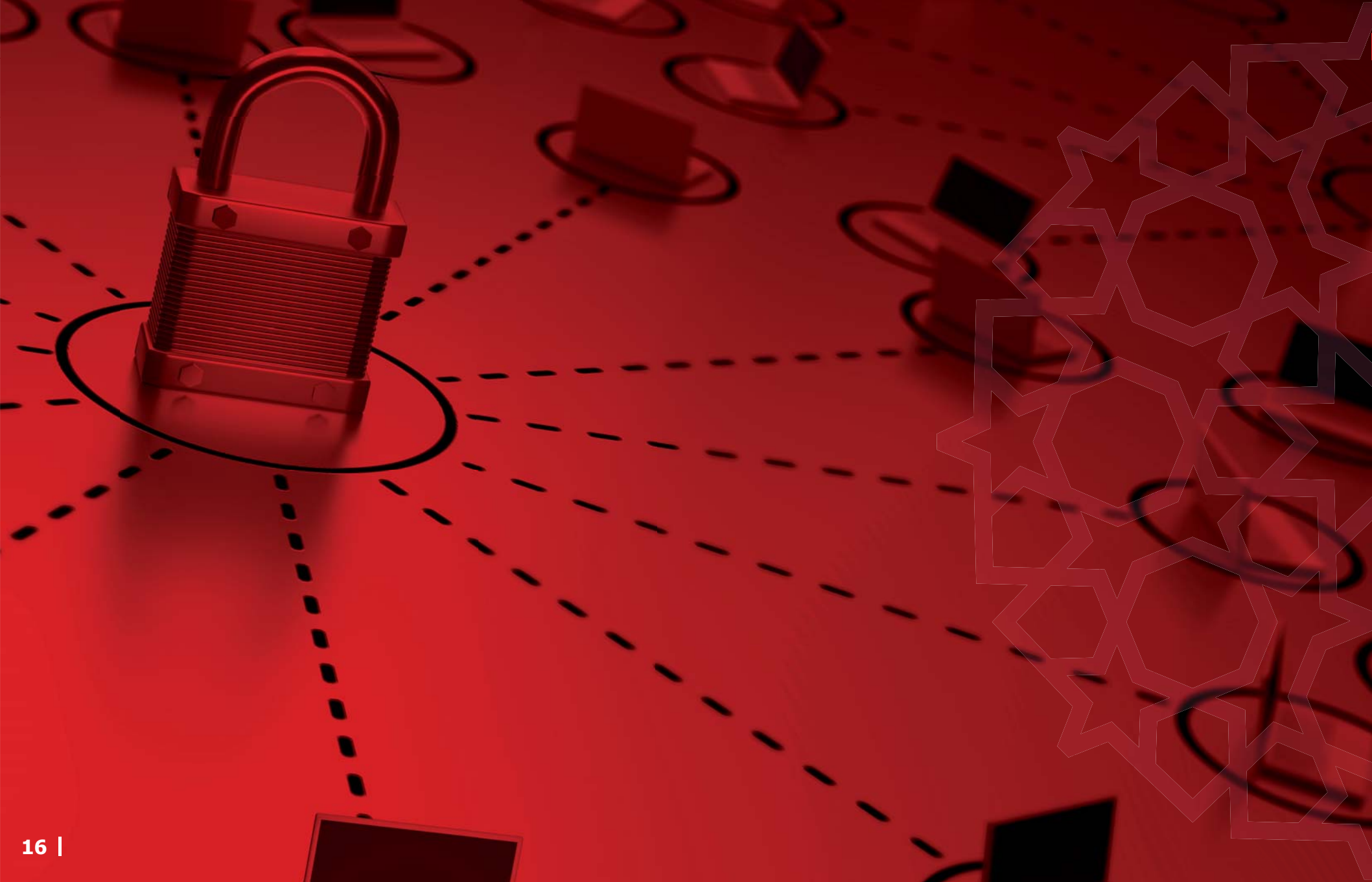
Anycast Round Table

A última sessão do *Tech Day* teve o formato de "mesa-redonda", e foi moderada por Jacques Latour do ccTLD .CA. Participaram três ccTLDs (.CA, .CZ e UK), três organizações com soluções comerciais (NetNod, Cloudflare e DYN) e por último uma organização sem fins lucrativos que disponibiliza de forma gratuita o serviços de Anycast (a PCH).

Os principais destaques vão para a apresentação das infraestruturas de servidores de resolução de nomes e respetivas soluções Anycast dos ccTLD's participantes, Jacques Latour do .CA, Jaromir Talir do .CZ e Chris Griffiths do .UK.

Patrik Faltstrom apresentou resultados das observações efetuadas nos sistemas da NetNod. Olafur Gudmundsson apresentou os serviços Anycast da Cloudflare. Andrew Sullivan fez uma apresentação comercial da solução da DYN. Bill Woodcock apresentou a solução de Anycast da PCH e um conjunto de melhores práticas que devem ser consideradas na implementação de soluções Anycast.


ICANN | 55 • DNSSEC



O Workshop DNSSEC organizado pelo ICANN Security and Stability

Advisory Committee (SSAC) e com contributos do programa Deploy360[9] da Internet Society, ocorreu no dia 9 de março. Dan York da Internet Society iniciou a sessão com a apresentação dos últimos números referentes à implementação de DNSSEC em todo o mundo. Uma vez mais, os dados apresentados foram recolhidos com a ajuda de Geoff Huston da APNIC, e do seu projeto de recolha de dados estatísticos através de anúncios do Google. Estes dados estão disponíveis online em: "http://stats.labs.apnic.net/dnssec/XA?c=XA&x=1&g=0&r=0&w=7&r=1".

Em termos globais observa-se um aumento continuou da validação das consultas DNS com DNSSEC, atingindo o máximo de 15,7% nos últimos dias de 2015. A média global dos últimos 2 anos, situa-se nos 13,35%. Em termos regionais o local onde se observa a maior taxa de validação DNSSEC é paradoxalmente em Africa, mais especificamente na África Oriental com 34,28%, no entanto esta situação justifica-se pela elevada utilização do serviço público de resolução DNS da Google, que garante 27,04% das consultas validadas com DNSSEC.

A utilização da expressão antagónica justifica-se porque Africa é ao mesmo tempo o continente com o menor número de ccTLD's assinados com DNSSEC, sendo os mais recentes o .BW do Botsuana em dezembro de 2015 e o .MA de Marrocos no próprio dia do workshop DNSSEC no ICANN. Estes dados também podem ser consultados online no site de Rick Lamb do ICANN em https://rick.eng.br/dnssecstat/ccmap.html.

Por último, uma referência à agenda de eventos relativos publicada pela iniciativa *DNSSEC Deployment* e disponível em https://www.dnssec-deployment.org/events/.

Os recentes valores baixos observados nos dados de Geoff Huston, nomeadamente em setembro, estão relacionados com dificuldades na medição devido a alterações introduzidas pela Google na sua solução de anúncios.

Implementação de DNSSEC em termos globais

[9] http://www.internetsociety.org/deploy360/

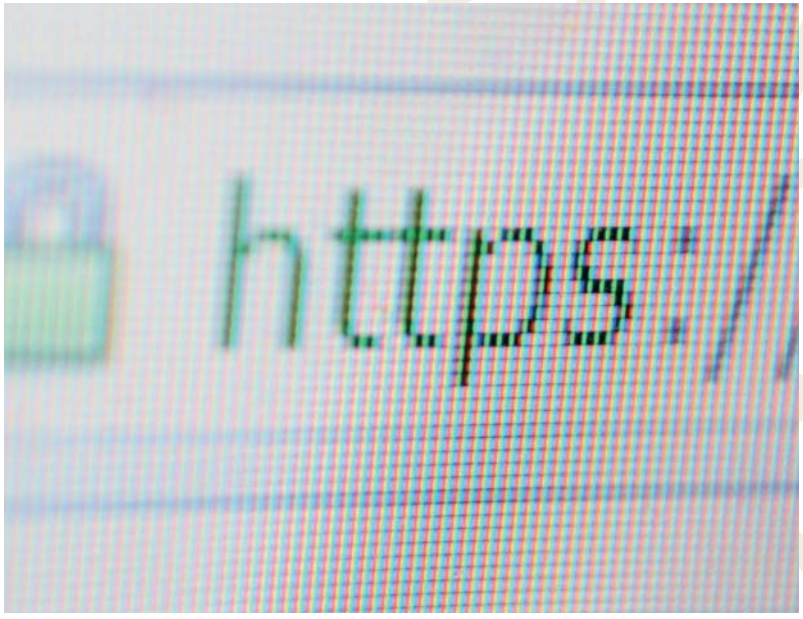
'Sunset' of the DNSSEC Lookaside Validation Registry (DLV)

Victoria Risk do Internet Systems Consortium (ISC) fez uma atualização do processo de descontinuação do serviço DLV (DNSSEC Look-aside Validation).Esta solução foi criada em meados de 2006, para validação das consultas DNS com DNSSEC, quando a raiz da Internet ainda não estava assinada com DNSSEC, processo que ocorreu 4 anos depois, no início de 2010. Ou seja, tratou-se de uma solução de apoio aos domínios de topo pioneiros a adotar DNSSEC, como o .PT.

Como mais de 70% dos domínios de topo ccTLDs e GTLDs, já estão assinados, existe uma ideia generalizada de que o DLV já cumpriu a sua missão, e como tal deverá ser descontinuado, no entanto algumas entidades continuam a ver esta solução como uma alternativa para validação DNSSEC. No início de 2015, durante a 52ª reunião do ICANN em Singapura, o ISC anunciou a intenção de descontinuar este serviço. A estratégia passava por reduzir ao mínimo, o tráfego DNS para este sistema e posteriormente remover as zonas DNS aí configuradas. Em junho de 2015 o ISC iniciou o processo, solicitou aos respetivos responsáveis, a remoção dos domínios configurados no DLV com problemas técnicos, no entanto rapidamente foi confrontada com feedback de que o DLV é uma solução necessária para os domínios lá configurados porque é a única forma de os manter assinados com DNSSEC.

Como consequência o ISC adiou o processo em 6 meses, prevendo agora a remoção completa dos domínios configurados no DLV em julho de 2017, ao fim de 2 anos dos responsáveis dos domínios terem sido notificados. Não obstante, o ISC já conseguiu remover 800 domínios no DLV, permanecendo ainda 2080 domínios ativos, e reduziu o tráfego DNS de 8.000 qps (consultas DNS por segundo), para menos de 4.000 qps.

Em suma, a posição do ISC é a de que o DLV foi criado para incentivar o uso de DNSSEC, apoio os domínios inovadores na implementação de DNSSEC como o .PT, e por último, o DLV não deve ser a solução para as dificuldades que o DNSSEC enfrenta atualmente.



DNSSEC Activities in the African Region

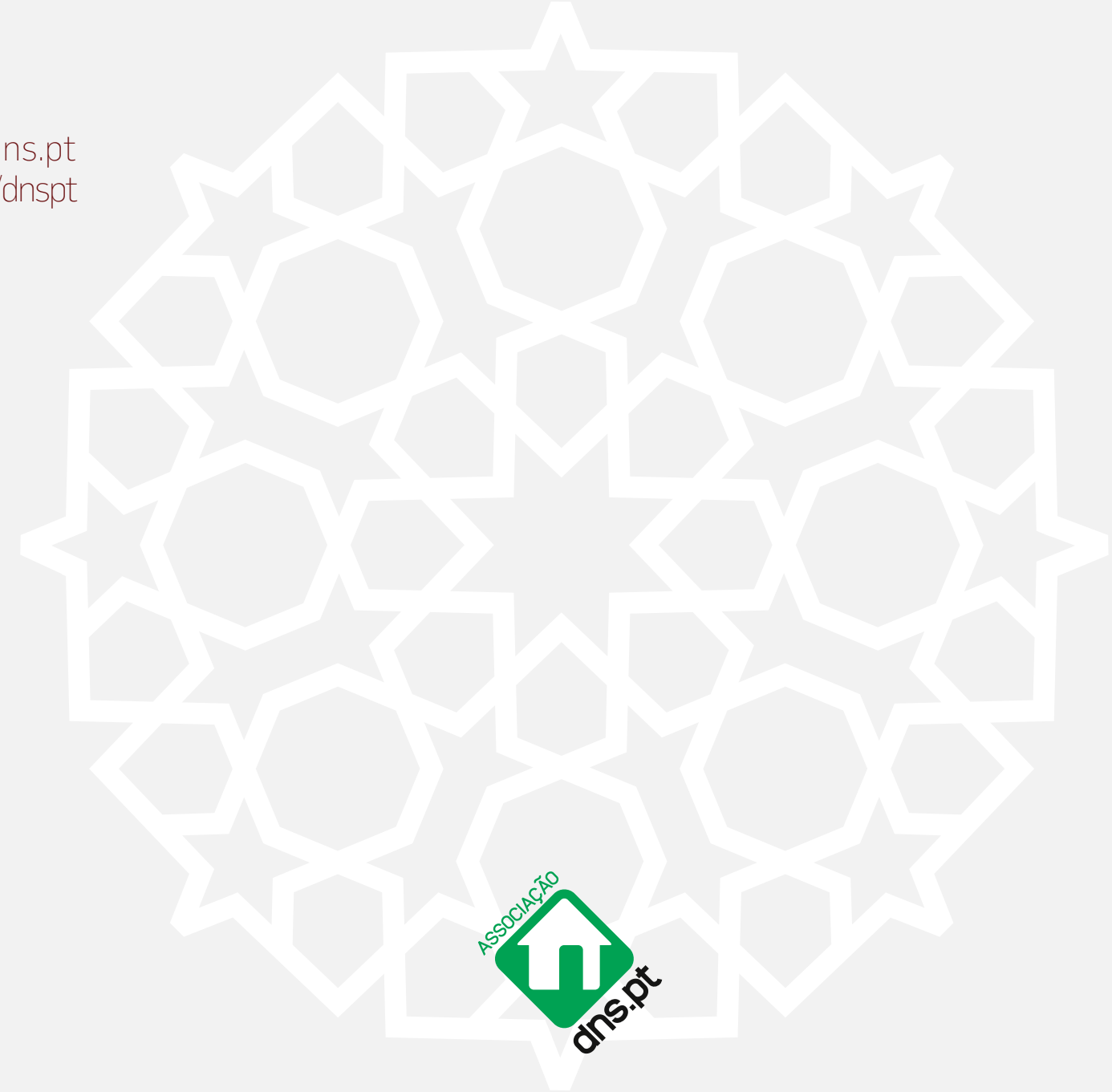
Os workshops DNSSEC do ICANN têm a particularidade de incluir na agenda, um painel de apresentação/discussão das atividades DNSSEC desenvolvidas na região anfitriã. Mark Elkins do ccTLD .ZA da Africa do Sul, foi o moderado da sessão em Marraquexe, onde destacamos desde já a participação de Sara Monteiro do DNS.PT que relatou o trabalho que o .PT tem vindo a desenvolver nesta área, junto das entidades registries análogas ao DNS.PT, de Angola, Cabo Verde, Guiné Bissau e Santo Tomé e Príncipe. Foi ainda dado a conhecer, a missão da Associação de ccTLDs de língua portuguesa LusNIC, que agora assume os trabalhos de cooperação já existentes e reforça a cooperação com um grupo mais alargado de países de língua portuguesa, como Moçambique, Brasil e Timor-Leste.

Alain Aina, consultor do ICANN no âmbito da iniciativa *Africa DNSSEC Roadshow*[10] fez um ponto de situação dos trabalhos quem têm sido desenvolvidos nesta região. Esta iniciativa faz parte do plano *ICANN's Africa strategy*[11] para a implementação de DNSSEC nos ccTLD's de Africa.

Outros temas a debate, incluíram a experiência da AfriNic, o Regional Internet Registry (RIR) da região, que efetuou a migração da sua solução DNSSEC com sucesso. Dani Grant da CloudFlare falou dos desafios que enfrenta ao usar DNSSEC em larga escala. Uma matéria que se encontra atualmente em discussão, e que foi discutida em Marraquexe são os algoritmos de encriptação de Criptografia de Curvas Elípticas no DNSSEC. Por último Geoff Huston da APNIC, e membro da equipa de desenho da solução de Rollover da chave Key Signing Key (KSK) do domínio raiz "root", fez um ponto de situação dos trabalhos e referiu os desafios deste processo.

[10] http://dnssec-africa.org/index.php
[11] http://africanncommunity.org/africastrategy/icann-aswg/

dns.pt
dnssec.pt
facebook.com/dns.pt
pt.linkedin.com/in/dnspt



Produção: abril 2016
Grafismo: dns.pt