ICANN83 | Fórum de políticas – Sessão do GAC sobre Segurança e Estabilidade
Quarta-feira, 11 de junho de 2025 – 9h às 10h15 CEST

DAN GLUCK

Bem-vindos a sessão do GAC sobre Segurança e Estabilidade, 11 de junho, quarta-feira, 9 horas. Isso se rege pelos padrões de comportamento esperados da ICANN. Durante essa sessão perguntas e comentários vão ser lidos em voz alta se forem apresentados de forma adequada no chat do Zoom. Haverá a interpretação nos seis idiomas oficiais da ONU e o português. Se quiserem falar durante a sessão, por favor, levante a mão na sala do Zoom. Se você desejar falar durante a sessão, por favor, levante a mão na sala do Zoom. Quando for chamado, o participante receberá permissão para ativar o microfone. Solicitamos que, ao falar em um idioma diferente do inglês, diga seu nome para registro e informe o idioma em que irá se expressar. Por favor, fale em um ritmo adequado para permitir uma interpretação precisa. Agora passo a palavra ao vice-presidente do GAC, Marco Hogewoning.

MARCO HOGEWONING

Bom dia a todos. Hoje vou presidir esta sessão porque o nosso presidente, Nico, está desfrutando do seu café e está agora com algumas ocupações. Vamos falar sobre algum dos projetos que está fazendo esse SSAC. Também temos Christian Hesselmann, de

	SDNLabs para explicar sobre a computação quântica e como age em DNSSEC. Antes de começar, talvez possamos fazer uma rodada de apresentações para que saibam quem está na mesa. Sou Marco Hogewoning, vice-presidente de Países Baixos.
MAARTEN AERTSEN	Bom dia. Meu nome é Maarten Aertsen e sou membro do SSAC.
WARREN KUMARI	Oi, eu sou Warren Kumari, também membro do SSAC.
GREG AARON	Sou Greg Aaron, do SSAC.
RAM MOHAN	Eu sou Ram Mohan, também sou do SSAC e o presidente do SSAC.
CRISTIAN HESSELMAN	Cristian Hesselman. Estou na SIDN, o registro do .NL, o domínio de topo dos Países Baixos.
MARCO HOGEWONING	Bom, passamos a palavra para Ram, para os primeiros comentários.

RAM MOHAN

Vamos falar sobre acesso de dados de registro de domínio. O que queremos fazer? Queremos garantir de compartilhar com o GAC o nosso objetivo. Queremos garantir que toda a política correspondente ao acesso aos dados de registro do gTLDs esteja bem definida, seja robusta e que abranja as necessidades da internet mundial, da comunidade global da internet e que a proteja das ameaças à segurança. Isso pode ser conseguido com um sistema de acesso que siga uma estrutura com um mecanismo expeditivo que permita manejar os pedidos de informação, sobretudo aqueles que são urgentes de forma expeditiva.

Que as políticas, quanto a tempos de resposta e como, que, onde, estejam claramente definidas e sejam aceitas dentro da comunidade. Também acreditamos que a organização da ICANN deveria continuar compartilhando indicadores sobre as solicitações de dados que chegam para pedir dados de registro de domínios. E pensamos que o acesso aos dados de registro é importante, é algo fundamental dentro da segurança e estabilidade.

E nós demos a nossa opinião ao EPDP, que se encarrega desse tema, desse tópico, mas queremos dizer que essa não é uma área que esteja em conflito com as necessidades em termos de privacidade. Temos as necessidades de privacidade abordadas de forma certa, mas há uma preocupação que tem a ver com a estabilidade e queremos garantir que o processo através do qual sejam realizadas essas modificações na comunidade, considerem os princípios que vocês veem aqui, elencados nesta tela. Queremos

dizer isso, e se tiverem perguntas ou comentários, estamos à disposição.

MARCO HOGEWONING Bom, acho que não sei se temos alguma pergunta, ainda é cedo. Não estou vendo nenhuma mão levantada aqui na sala, nem no Zoom. Então, talvez possamos continuar com o próximo assunto, que acho que faz referência ao software de código aberto. Maarten?

MAARTEN AERTSEN Estamos trabalhando num tema que pode ser familiar para alguns de vocês, que é o software livre de código aberto. O software que pode ser usado de forma livre, pode ser compartilhado, modificado, e estamos tentando determinar o papel desse software dentro do ONS global.

Mas não há um estudo exaustivo para essa comunidade, esse software livre de código aberto tem algumas características quanto ao seu desenvolvimento e governança, e apesar de que em algumas partes do mundo as pessoas discutem sobre infraestrutura, software, e a confiabilidade, achamos que é importante tornar visível a função desse software, suas características, para garantir que quando houver um debate em matéria de política, seja considerado.

Esse trabalho tem dois objetivos, queremos dar visibilidade a essa dependência crítica e também queremos que as características

desse software sejam visíveis, informar algumas das suposições que nós fazemos sobre software em geral, mas talvez não se apliquem nesse tipo de software. Então, essa é uma apresentação para adiantar o que vem depois.

Basicamente, nos concentramos em quatro áreas com uma enquete para descrever o estado de situação, ver que se passa do lado do registro de domínio e também do lado do DNS, onde são publicadas e recuperadas mapeamentos para ter uma ideia de como está a situação agora. Também analisamos as características desse software, inclusive o modelo de desenvolvimento, que não é o mesmo utilizar com outros tipos de software, e depois contrastamos essa análise do software livre de código aberto quanto às suas características com o software que é popular em DNS, aquele que nos preocupa nesse contexto.

A terceira parte tem a ver com esclarecer alguns supostos que nós aplicamos na prática que talvez não sejam viáveis aqui e esclarecer se há algum conceito errado. Depois, tentamos enumerar os fatores de risco que têm que ser considerados quando se formulam políticas ou regulamentações. Tem a ver com o desenvolvimento, mas também com as operações desse software.

Basicamente, essas são as áreas nas quais estamos nos concentrando. E, em Mascate, esperamos contar mais ao respeito porque esperamos publicar esse relatório nos meses posteriores a essa reunião de hoje. Como para adiantar, achamos que o uso do software livre e de código aberto no sistema de nomes de domínio

e com os registros é uma fortaleza, mas também queremos oferecer algumas diretrizes gerais a respeito desse tipo de software para considerar seus riscos. Fico à disposição para qualquer pergunta.

MARCO HOGEWONING Foi um avanço breve, conciso. Tem alguma pergunta para Maarten sobre esse trabalho? A Índia levantou a mão.

SAJID Essa é uma pergunta para o Ram Moham. Compartilhou os objetivos de que os dados de registro deveriam estar disponíveis num prazo de 24 horas, mas já faz dois anos que estamos tentando que esse prazo seja acordado, mas, pelo momento, não temos nenhum acordado. Embora seja estabelecida a urgência, em várias oportunidades se disse, tanto no GAC quanto no SSAC, esse é um processo muito extenso, que vai pelo caminho da autenticação e da política por outro.

Mas o que pensam, como presidente do SSAC, e também a pergunta pertinente ao vice-presidente do GAC, poderia haver uma declaração conjunta dos dois comitês a respeito de acordar um prazo para esse acesso aos dados, assim que possível?

RAM MOHAN Estamos de acordo de que, para os pedidos urgentes de informação, o processo deveria estar muito claro, e acho que certas deliberações estão em andamento entre as partes que são

responsáveis pela implementação dessas mudanças. Não posso falar em nome do SSAC em seu conjunto, teria que consultar com seus membros, mas fomos muito claros quanto aqui se há algo considerado urgente, tem que ser tratado como tal, e as respostas devem ser dadas de forma expeditiva, não pode insumir muito tempo. Se ajuda que façamos algo de forma conjunta com o GAC, estamos abertos a considerá-lo, a enfatizar a importância dessa questão, pensamos que é um assunto importante. E, em parte, temos que ter bem claro que urgente significa urgente, não é a operatória habitual.

MARCO HOGEWONING Obrigado, Ram, por essa resposta, estou de acordo. Obviamente, como vocês sabem, o GAC mencionou as solicitações urgentes nos últimos cinco comunicados, pelo menos os que eu lembre. Também o assessoramento a alguns colegas nas equipes reduzidas que estão tratando também esse assunto. E da minha perspectiva, vamos avançando. Estou de acordo com a sua observação sobre aqui, essas solicitações urgentes não estão avançando urgentemente, mas estamos alinhados com o Ram e tenhamos isso em mente e consideremos que um esforço conjunto poderia ajudar a que tudo avance mais rapidamente. Então, em algum momento, voltaremos a ver isso. Não sei se há perguntas. Russell, sim.

RUSSELL WORUBA

Fala, Russell, de Papua Nova Guiné. Obrigado, colegas, obrigado aos colegas do SSAC que estão fazendo um trabalho excelente, sou seu seguidor e acho que é uma força que recebemos gratamente. Acho que muitos dos países nas regiões subatendidas dependem enormemente do software de código aberto para gerenciar o DNS a nível de ccTLDs. E agora, com todo o panorama e as mudanças que se enxergam, estamos atentos aos resultados desse estudo. Terão alguma base para nos dizer qual é a situação nas diferentes regiões? Obrigado.

MAARTEN AERTSEN

Obrigado pela pergunta. Posso adiantar alguma coisa. Com relação a essa enquete do panorama atual, onde tentamos obter dados duros de quem usa o quê. Acho que no rascunho atual, prevemos dizer que o DNS global utiliza software de código aberto. Não são só vocês, temos estatísticas para apoiar isso. No espaço dos ccTLDs 20 de 25, operadores utilizam esse software.

Se somam o espaço dos ccTLDs, são 9, e são 9 de 12 que utilizam esse tipo de software. Então, acho que esse é um dos valores que pode oferecer esse relatório, trazer à tona para um público mais amplo, e aqueles que são novos na tecnologia, que o software está em toda parte, e esperamos dar essa informação, porque em algumas regiões vimos que o software está sendo regulado e que esse software de código aberto não está sendo considerado, e talvez na estratégia atual, na financiação, também não seja correta.

MARCO HOGEWONING A Alemanha abriu a palavra.

RUDY NOLDE Queria perguntar qual o conselho que tem para formuladores de políticas, porque no último slide falavam sobre algumas diretrizes, e acho que avançou um pouco, mas como sou impaciente, quero perguntar se talvez pode dizer de forma preliminar, vão com essas diretrizes? Para nós, formuladores de políticas?

MAARTEN AERTSEN Não quero roubar tempo dos meus colegas. Vou tentar ser breve. Como estamos pensando? Queremos deixar visíveis alguns dos conceitos errados, um que é bastante natural, é que podem ser utilizadas relações contratuais para ter um mecanismo no âmbito da política. Regulamos os operadores de estrutura crítica na região, mas depois se tornam críticos os fornecedores que vão colocar requisitos aos seus próprios fornecedores. Isso pode funcionar para materiais físicos, mas não quando é descarregado da internet, porque não há uma cadeia lá.

Essa é uma concepção errada. Na prática, não funciona assim, porque há muito software que se desenvolve e é mantido por um grupo específico. Mas, quando se trata do uso, isso vai além da existência desse contrato de suporte. Então, do ponto de vista do que podemos assessorar, talvez possamos oferecer alguns comentários, reflexões nesse âmbito em particular como gerenciar

os desenvolvedores nesse sentido e também se impor os requisitos aos operadores.

Isso poderia restringir a sua capacidade de escolher o software melhor da sua classe e talvez isso poderia ser que resulte que seja o melhor tipo de software. Talvez não possa ser possível cumprir com a política que esperávamos, mas o caminho é esse. Primeiro temos que publicar o relatório e depois poderia falar com mais informação a respeito.

MARCO HOGEWONING Bom, eu acho que vamos esperar o relatório, a publicação desse relatório, e depois continuaremos com esta análise. Agora, vamos passar ao próximo assunto, que é de muito interesse para mim e que trata o bloqueio do DNS. E vamos dar uma nova análise, uma perspectiva.

GREG AARON Vamos apresentar o documento 2, na verdade, que o SSAC preparou há 12 anos e um novo documento que atualiza a informação. Consideramos oportuno atualizar essas duas publicações prévias porque há muitos exemplos sobre o bloqueio do DNS a escala mundial. E vemos os resultados desse relatório, dessa mudança.

Também se desenvolve a nova tecnologia que trata o bloqueio do DNS e como as pessoas podem acessar recursos na internet. Trabalhamos também 20 membros do SSAC nessa nova iniciativa

e veremos o que é o bloqueio do DNS. Quando as pessoas estão perante o computador e querem acessar um website, colocam o endereço, o nome de domínio desse website e enviam a consulta a um resolutor do DNS, o resolutor recursivo que está administrado por seu ISP.

Esse resolutor recursivo traduz esse endereço IP do website ao qual vocês querem acessar ou chegar e o DNS reconhece qual o website que vocês querem chegar e dessa forma acontece a conexão. Normalmente, esse processo é praticamente instantâneo, mas o resolutor recursivo pode bloquear um nome de domínio. Isso significa que o resolutor vai dar uma informação diferente da esperada.

Basicamente, isso acontece de duas formas. Primeiro, o resolutor recursivo pode dizer que aquele domínio que estão buscando não existe, quando, na verdade, sim, existe. Por exemplo, a Wikipédia. Querem acessar a Wikipédia e não podem? Isso é o que acontece. E também pode acontecer que vocês são levados, digamos, a outro destino da internet e não é aquele que vocês queriam. Ou seja, o resolutor recursivo diz uma coisa inesperada. Ou, inclusive, está mentindo, como falam alguns, porque não dá a resposta que, sim, existe no DNS.

Então, o bloqueio do DNS é uma técnica, uma ferramenta, e que, como toda ferramenta, pode ser utilizada com diferentes finalidades. Pode ser utilizada de forma correta ou de forma inesperada. Um martelo, por exemplo. Podemos usar um martelo

para construir uma casa ou dar na cabeça de alguém, e isso não seria o esperado.

Então, basicamente, essa ferramenta está desenhada para que as pessoas não possam acessar os conteúdos ou algum serviço em particular. E isso não só afeta os websites, mas também os correios eletrônicos, o gerenciamento de redes, tudo o que acontece no DNS. Então, se o resolutor do DNS for Gandalf, essas referências, nós adoramos essas referências no DNSSEC. Isso é o que diria o recursor recursivo. Então, o bloqueio do DNS se utiliza com diferentes finalidades. Então, a finalidade é também importante.

Em primeiro lugar, é utilizado com fins de segurança. O resolutor... Opa. Desculpem. Que efeito dramático. Caiu a luz. Bloquearam a eletricidade. Enfim, vou continuar. O resolutor do DNS pode estar configurado de forma tal que as pessoas não possam acessar sites com phishing, malware, sites enganosos. Este é um serviço beneficioso, positivo, claro, e todos nós, de alguma forma, estamos protegidos pelo bloqueio do DNS.

Os buscadores web, por exemplo, têm um sistema que alerta quando estamos por acessar um website que comete phishing, por exemplo. Então, esta é uma questão endêmica em múltiplos sistemas. Está muito presente. E, em termos gerais, a ideia é proteger e ajudar as pessoas. E se faz, geralmente, a nível local. Por exemplo, vocês querem que uma empresa ajude com a segurança da sua rede e trabalham dessa forma.

Também é bloqueado o DNS para bloquear conteúdos. Por exemplo, a sua biblioteca local talvez não permita que acessem alguns conteúdos em particular. Por exemplo, sites de pornografia ou de apostas, porque a essa biblioteca chegam crianças, ou podem acessar crianças. Também, a nível de empresas, se bloqueiam conteúdos porque algumas empresas não querem que seus funcionários tenham acesso a websites de apostas ou às suas contas de rede social enquanto estão trabalhando na rede da empresa.

E, no caso, a empresa tem uma política determinada ao respeito. Mas há uma coisa que é muito controversial. Utilizar o bloqueio do DNS para que as pessoas não tenham acesso a conteúdos, principalmente se se bloqueia o DNS a escala nacional. Por exemplo, pessoas de todo um país não podem acessar tal ou qual website, não podem ver tal ou qual conteúdo.

Então, por isso, queremos apresentar esta informação àqueles que formulam as políticas aos membros do GAC, por exemplo, porque estas decisões afetam muitas pessoas. Às vezes, o bloqueio tem fundamento numa lei. Alguns países, por exemplo, não permitem que os seus cidadãos visitem websites que têm pornografia infantil para proteger as crianças e também para proteger os cidadãos desse país.

Os países têm uma lista desses domínios e disponibilizam os seus ISPs. Mas há uma coisa mais controversial ainda. Em alguns países, é bloqueado o DNS para acessar conteúdos que refletem opiniões

políticas. Então, aí existe a censura, ou surge a censura. Queremos fazer uma diferença entre suspensão de nomes de domínio e bloqueio do DNS. Em ambos os casos, é bloqueado o acesso ao conteúdo.

No entanto, no bloqueio do DNS, não se elimina o conteúdo. Outras pessoas podem acessar esse conteúdo. Mas, quando é suspenso um domínio, ele é retirado da internet, ou seja, deixa de funcionar na internet. Isso se faz no mundo todo para prevenir alguns países ou o uso indevido, o phishing, porque essas medidas obedecem às resoluções da justiça.

Aqui vemos uma imagem, por exemplo, que indica que um website foi apreendido, digamos, como resultado de uma decisão judicial. Às vezes, então, é retirado por completo ou se faz um reencaminhamento do website e se coloca em outro servidor de nomes. Mas o objetivo final é o acesso a esse site.

Aqui vemos um resumo do documento. Nesse documento, o SSAC fala sobre as técnicas utilizadas para bloquear o DNS, os motivos pelos quais isso acontece. Em alguns casos, talvez as pessoas não estejam de acordo com os casos práticos, porque o que é legal em um país talvez não seja em outro. Algumas pessoas não estarão de acordo com os fundamentos de uma resolução judicial, e cada caso apresenta uma situação diferente.

WARREN KUMARI

Como disse Greg, o bloqueio do DNS é uma ferramenta que tem fortalezas e fraquezas. Temos que entender como funciona para justamente ficarmos isolados do conteúdo. O que se faz é colocar listas nos resolutores recursivos do que pode ser apresentado ou mostrado ou não. Isso aplica aos usuários daquele resolutor recursivo em especial.

Com isso, o usuário, se vai para outro resolutor recursivo, vai evitar esse bloqueio. Então, aqui vemos um usuário que envia suas consultas a um resolutor padrão do seu ISP. Eles procuram um nome e esse nome é aprovado. Se resolve a busca de forma normal. Mas, se está numa lista de bloqueio do DNS, às vezes a resposta diz que o nome não existe ou também o resolutor recursivo vai nos reencaminhar na busca.

Agora, se o usuário vai para outro resolutor recursivo onde não há bloqueio, então vai poder acessar esse conteúdo da internet de forma normal. Como fazem os usuários para utilizar um resolutor diferente? Há uma série de quantidades de resolutores públicos que são utilizados por uma grande quantidade de usuários. Aqui vemos que aproximadamente 21% dos usuários utilizam os resolutores públicos conhecidos a nível mundial.

Aqui vemos alguns exemplos como o DNS público de Google, Cloudflare tem também seu próprio resolutor e Quad9. Mas também há resolutores dos governos, por exemplo, DNS4EU, que é um serviço público de resolutores. Então, isso é fácil, inclusive

para os usuários que não têm conhecimento técnico, eles podem configurar seus resolutores e ver para onde vão dentro do DNS.

Nos últimos anos, foram utilizados serviços de streaming. Se os senhores ou senhoras têm utilizado esses serviços, devem ter visto publicidade de VPN com marcas muito conhecidas no mercado que oferecem essas VPN, que oferecem benefícios, melhoram a nossa privacidade, entre outras coisas. Mas também, nesses anúncios, fica claro que servem para evitar as restrições geográficas.

Então, se viajarmos e queremos ver alguma coisa em uma plataforma de streaming do nosso país de origem, podemos nos conectar a um VPN que apresente na internet que estamos naquele tal país. Também, se estão em um país onde querem ver um conteúdo que justamente não está à disposição no nosso país de origem, podemos justamente comprar um serviço de VPN e escolher outro país. Então, a internet pensa que estamos ali e podemos ver o conteúdo.

Isso significa, entre outras coisas, que estamos utilizando um conjunto diferente de resolutores recursivos, e, portanto, a internet pensa que não estamos no tal país. Ou seja, se há um bloqueio em alguns resolutores recursivos, podemos evitar esse problema com o uso do VPN. Agora, vamos passar a palavra a outro panelista.

MAARTEN AERTSEN

Muito bem. O que pode dar errado ou nem tão certo? Às vezes, há um bloqueio excessivo quando o bloqueio é muito amplo. Por exemplo, podemos bloquear um domínio de terceiro nível, depois um de segundo nível e também a nível do TLD. Se o bloqueio é muito amplo, talvez se evite o acesso a mais de um destino ou mais de um website. E isso é um problema. Para aqueles que querem acessar esses websites, que talvez não sejam problemáticos, por assim dizer.

Isso acontece quando fazemos um bloqueio no site errado. Há muitos casos práticos, muitos exemplos no documento. Então, nós sugerimos a sua leitura e que reparem nesses casos práticos. Há um antecedente de bloqueio excessivo. Por exemplo, a Itália oferece alguns nomes de domínios ao seu ISP e, sem querer, incluíram um domínio nessa lista utilizado para infraestrutura. Então, isso foi um bloqueio excessivo que derivou no bloqueio de Google Docs para os usuários da Itália por um breve período até que alguém percebeu o erro.

Esse erro gerou inconvenientes para os usuários que não podiam acessar conteúdos que não eram problemáticos de forma alguma. Esse é um dano colateral. Se não trabalhamos bem ou se não fazemos bem o bloqueio, vamos afetar pessoas que não deveriam ter sido afetadas. Como disse Warren, as pessoas podem evitar um bloqueio.

A cada vez que há um bloqueio, se deve supor que um usuário vai achar uma via alternativa, principalmente se tem um motivo

suficiente. Pode usar seu VPN, outros resolutores. De fato, há tecnologias que permitem que os usuários acessem a conteúdo ou façam com que o conteúdo continue estando disponível. O bloqueio do DNS é uma questão gradual. Se alguém supõe que enviamos um domínio e mandamos uma ordem a um ISP no país, vai-se solucionar o problema? Mas para alguma quantidade, sim, mas para outras, não.

WARREN KUMARI

Bom, quando é bloqueado um domínio, o resolutor recursivo pode responder de duas formas. Um, o domínio não existe, e dois, vemos que o resolutor recursivo reencaminha o usuário para outro destino. Isso, ao nosso ver, é bastante perigoso, por quê? Se o usuário está tentando chegar a um site e é redirecionado para outro site, o buscador web vai nos dar um alerta, vai nos dizer, "você quer chegar a tal site", mas, em realidade, está chegando a outro.

Então, vamos receber essas mensagens de alerta que têm repercussões em matéria de segurança. Às vezes, ignoramos esses alertas, mas, outras vezes, pode ser que ignoremos e estejamos tentando chegar ao website do nosso próprio banco. Então, por favor, se vão bloquear o DNS, não façam um redirecionamento.

E agora, acho que vamos passar para recomendações. Muito bem, eu vou continuar com a apresentação. Como já dissemos previamente, o bloqueio do DNS é uma ferramenta e como qualquer uma delas pode ser utilizada para o bem, mas se não

sabemos utilizá-la ou não conhecemos as instruções, podemos resultar prejudicados. Então, se vão utilizar o bloqueio do DNS, garantam saber como funcionam e quais as consequências colaterais.

GREG

Além disso, o SSAC recomenda que, se vamos fazer com que seja obrigatório um bloqueio do DNS dentro de uma empresa em nível nacional ou dentro de um ISP, temos que seguir essas diretrizes. Em alguns casos, essas diretrizes se baseiam no princípio médico de não provocar danos. Então, temos que ver esse bloqueio, como é que vai conseguir os nossos objetivos e se serve para isso. Talvez haja algumas medidas alternativas. Temos que pensar se o bloqueio vai nos ajudar ou não vai ser suficiente?

Temos que ter uma política clara do que é que queremos bloquear e como vamos fazê-lo. E temos que ter procedimentos bem definidos para analisar o que incluímos na lista de bloqueio e minimizar o risco. E também saber como corrigir um erro. Não recomendamos políticas e procedimentos específicos, porque dependem dos seus próprios objetivos.

Mas esse é um princípio importante. Devemos implementar isso de forma tal que seja minimizado o bloqueio excessivo ou o dano colateral para os usuários. Por exemplo, numa empresa, os seus empregados, que poderiam se ver prejudicados e, por último, não

devem ser afetadas as pessoas que estão fora da sua responsabilidade administrativa.

Por exemplo, na Europa, há muitos países e alguns dos ISPs europeus têm clientes em mais de um país. Então, se estão no país A e o ISP tem clientes no país A e B, o que se passa se o ISP recebe uma ordem do país A de fazer um bloqueio? Como bloqueia esse ISP ou DNS sem afetar os clientes que tem no outro país, fora da sua jurisdição territorial? Vemos as fronteiras nacionais no mapa, mas a internet não se correlaciona com essas fronteiras. Então, cuidado. Tem que ter cuidado de não afetar as pessoas que não têm direito de afetar.

WARREN KUMARI Vou ser rápido porque não temos tempo. A última recomendação tem a ver com os operadores do servidor recursivo que utilizam RFC para os códigos de erro estendido, que incluem o bloqueio. Acho que podemos receber perguntas.

MARCO HOGEWONING Bom, não temos muito tempo para perguntas. Muito obrigado. É um trabalho extremamente detalhado como parte do público ao qual vai dirigido. Agradecemos. Temos pouco tempo. Mas acho que, sim, podemos receber uma pergunta breve. E vejo que Papua Nova Guiné, no chat, fez um comentário. Não sei se quer fazer também a pergunta aqui.

RUSSEL WORUBA Obrigado, Marco. Como país, fomos convidados a participarmos em ensaios sobre o serviço de proteção de nomes de domínio. Então, queria falar sobre isso em particular e perguntar se poderiam dizer alguma coisa a respeito.

MAARTEN AERTSEN Sim, o serviço de proteção de nomes de domínio pode ser usado através do domínio de DNS. Esses resolutores públicos que mencionamos se encarregam dessa proteção contra o malware ou phishing, o bloqueiam para proteger os seus usuários. Essa é uma técnica que pode ser utilizada para proteger os usuários. Também dizemos que esse documento foi usado para fornecer informações no âmbito político, principalmente no Japão, estão considerando bloquear determinado conteúdo específico no país.

WARREN KUMARI Cloudflare é uma das organizações que oferece resolutores públicos e três endereços diferentes. Um é 1.1.1.1, onde não fazem bloqueio. Depois tem 1.1.1.2, para bloquear malware. Depois 1.1.1.3, que oferece mais proteção, bloqueia malware e outro tipo de conteúdo para adultos.

Então, nós dizemos, se vai se oferecer um serviço de proteção para um grupo maior, os usuários deveriam poder escolher o nível de proteção. Se a gente for pai, poderia escolher proteger contra determinado conteúdo. Pode usar o serviço de proteção de DNS que impeça a ver esse conteúdo. Mas talvez, se não estiver nessa

situação, pode optar para ver esse conteúdo. Poderia haver diferentes níveis de bloqueio para diferentes pessoas afetadas. Se a gente decide querer essa proteção, talvez seja mais manejável do que aquela que é imposta.

MARCO HOGEWONING

Há três pessoas que pediram a palavra. Vou encerrar a lista de intervenções aqui. Sejam breves um minuto para cada pergunta e resposta, se for possível, para termos tempo depois do outro assunto. Em primeiro lugar, temos Blaise.

BLAISE AZITEMINA FUNDJI

Fala Blaise Azitemina da República Democrática do Congo. Tem uma preocupação com as VPN, embora esteja agradecido pelo nível de segurança que nos oferece uma VPN. Ao mesmo tempo, da perspectiva de política, me preocupa a deslocalização, porque os países em desenvolvimento, lá muitos utilizam a VPN, não pela proteção ou segurança que ofereçam, mas, basicamente, para ocultar outro endereço de um país, para mostrar que estão em outro país, às vezes.

E, em ocasiões, essa é uma violação às políticas de segurança dos nossos países. Vemos plataformas de streaming que parecem ter achado uma solução, quando a gente se conecta através de uma VPN, de um proxy, vai dizer que não qualificam ou que não têm acesso. Então, qual é o equilíbrio entre a segurança, a proteção e, ao mesmo tempo, a exatidão da posição geográfica? Obrigado.

MAARTEN AERTSEN

Acho que o SSAC não considerou todas as consequências. Em verdade, as VPNs estão amplamente disponíveis, bem como outras ferramentas são utilizadas com bons propósitos e maus propósitos. Os delinquentes as utilizam para ocultar onde estão. A VPN aproveita as vantagens do funcionamento da internet e estão aqui para ficar. Algumas empresas mantêm listas de VPNs ou de IPs de VPNs conhecidas. Por exemplo, utilizam para qualificar os riscos do tráfico que provém desses endereços. Então, há ferramentas para detectar e entender o tráfico das VPNs.

WARREN KUMARI

E, se me permitirem adicionar, as VPNs estão desenhadas para ser vistas como um tráfico normal de internet. Então, em alguns lugares em que se tentou proibir seu uso em empresas ou países, parecem bloquear os grandes serviços de VPN, mas os usuários querem poder acessar. Então, eles vão para uma lista de VPNs com seguimento e talvez possa ser muito mais inseguro isso. Então, às vezes, há consequências negativas quando se tenta bloquear uma técnica que os usuários utilizam para chegar a acessar esse conteúdo. Vão achar a forma de acessar esse conteúdo.

MARCO HOGEWONING

Bom, podemos fazer as próximas perguntas. Sejam breves.

SUSHIL PAL

Acham que o DNS, que esse DNS EU pode ser uma solução? E as VPNs, sim, têm importância. Algumas que são conhecidas, mas os organismos de segurança estão procurando alguma forma de monitorizar as VPNs que não são conhecidas?

GREG

O que posso dizer com relação ao DNS 4 EU é que eles armaram o site, o website, com base na soberania. Então, em lugar de enviar o tráfico para resolutores comerciais grandes, agora oferecem esse sistema para que o tráfico esteja na Europa, através de DNS 4 EU. Agora, se os organismos de segurança procuram formas de monitorizar as VPNs desconhecidas, não sei.

MARCO HOGEWONING

Indonésia, última intervenção.

ASHWIN SASONGKO SASTROSUBROTO

Estava pensando nesse comentário sobre bloqueio e impactos negativos. O que acontece se não se permite acessar ao ciberespaço com o DNS? Só ao que quereremos. Por exemplo, se é .org, não permitimos e dizemos .com se é autorizado. Em lugar de bloquear, se bloqueia tudo e depois vai se autorizando o acesso ao DNS. Com certa aprovação.

WARREN KUMARI

Não sei se realmente isso seja viável. Há milhões de sites na internet. Então, escrever uma lista daquilo que sim pode ser visto

é bom, mas inclusive se fosse possível, tecnicamente não é possível nesses dias, bloquear todo o acesso ao DNS, a novas tecnologias, DNS sobre TLS, DNS sobre QUIC. Não está visível que a consulta seja uma consulta em si própria. Somente vê tudo como tráfico de internet. Então, não se pode desconectar o país da internet, porque afetaria outros fornecedores de serviços de internet, como Starlink, por exemplo. Então, muitos ficarão isolados.

GREG

E as tecnologias que mencionou Warren, basicamente, estão relacionadas com a criptagem. Com a criptografia, sim. Isso tem a ver com os usuários finais que estão fazendo as consultas. Por isso, essas tecnologias são tentativas para oferecer maior privacidade na internet.

MARCO HOGEWONING

Obrigado, peço desculpas. É muito interessante este tema e vejo que há muita interação. Então, vale a pena dar continuidade. Temos também o código QR para acessar o relatório completo. Então, por favor, dê uma lida. Está já publicado faz um tempo. Obrigado, Greg, Warren, Marteen. Se sintam livres de ficar por aqui. E quero agora passar ao que eu acho que é uma atualização sobre as conversas que tivemos sobre computação quântica e alguns dos riscos. Isso falamos em Seattle. Então, quero receber a Christian Hesselmann, de SIDNLabs, para que comente qual seria o impacto no DNSSEC e que nós, como representantes do governo, o que

podemos fazer para mitigar alguns desses problemas. Por favor, Christian.

RAM MOHAN

Antes disso, quero agradecer ao GAC por este convite. Agradecemos o convite.

CRISTIAN HESSELMAN

Obrigado, Marco. Com essa apresentação, vamos falar sobre a computação quântica DNSSEC e o impacto que essas futuras máquinas poderiam ter. No final dessa palestra, eu vou apresentar algumas ações sugeridas pelo GAC. O que aconteceu com os slides? Desapareceram, sumiram. A imagem que acabam de ver, eu vou continuar falando. Eu peguei do Centro de Computação Quântica da Alemanha, onde está se trabalhando basicamente numa fase experimental que parece quase que ficção científica.

Bom, aqui estamos. Próximos slides, sim. Então, em primeiro lugar, quais seriam as expectativas a respeito dos computadores quânticos? Eu não sou especialista em computadores quânticos, sim em sistemas distribuídos. Então, eu acho que os computadores quânticos, enfim, esse conhecimento tem os físicos, mas eu não sou uma dessas pessoas. É o que eu li a partir da bibliografia. As expectativas quanto aos computadores quânticos é que existam novos aplicativos, descobertas de novos fármacos, diferentes métodos médicos, a melhora da aprendizagem automática, o desenvolvimento de materiais revolucionários.

Mas, como disse Greg, pode ser utilizada a tecnologia de diversas formas. Então, esse é o exemplo do martelo. Podemos utilizar de forma positiva, mas também, de alguma forma, com alguns riscos. A desvantagem é que esses computadores podem quebrar os algoritmos criptográficos ou criptografados. Alguns poderiam ser os algoritmos para o DNSSEC, por exemplo, que se vejam afetados, que se utilizam para autenticar as mensagens de DNS e verificar a integridade de ditas mensagens.

Bom, outra vez sumiram os slides. Querem que continue? Esperamos os slides aparecerem? Muito bem, aí está. Voltamos. Então, os riscos dos computadores quânticos em termos do DNSSEC é que potencialmente poderiam alterar os algoritmos criptografados que utiliza a DNSSEC para verificar a autenticidade, a integridade e a resposta do DNS. Potencialmente, isso poderia encaminhar ou direcionar ou afirmar novamente a mensagem com uma senha comprometida, fingindo que as mensagens são reais, quando, na verdade, poderíamos chegar a lugares incorretos aos quais não deveríamos ir.

Aqui, supomos que todos vivemos na época pós-quântica, não seria agora, mas no futuro. Ou seja, tudo isso tem a ver mais com um ataque que não acontece agora, mas que poderia acontecer no futuro. Mas, em tempo real, poderia comprometer todas as senhas utilizadas para as firmas no DNSSEC. Mas os especialistas pensam que isso não vai acontecer até 10 ou 15 anos. Então, a pergunta seria, por que deveríamos trabalhar agora neste tema?

E a resposta é por quê. Substituindo os algoritmos criptografados no DNSSEC, isso leva muito tempo. Isso surge de um trabalho onde se vê o desenvolvimento de um algoritmo criptográfico no DNSSEC. Então, a partir da primeira versão preliminar, a ITF até a implementação completa, que aparece aqui na direita do quadro, desculpe, desde o início, na esquerda, até sua finalização, à direita do quadro, podem ver que há muitas atualizações, muito trabalho.

Então, se os computadores quânticos vão se transformar em uma realidade daqui a 10, 15 anos, temos que pensar que temos que, hoje, fazer alguma coisa no âmbito do DNS. Além da questão do tempo, temos um trabalho de implementação importante a fazer para o DNSSEC. Aqui podemos ver os países que assinaram com o DNSSEC os seus TLDs que estão na cor verde e já estão operacionais. Na cor verde e azul, 48% do mundo. E, à direita, podem ver a validação.

Este é um mapa que tem mais cor vermelha e âmbar, porque a validação dessas firmas tem um nível de adoção mais baixo. Então, há coisas que ainda devem ser aprovadas. Mas, como podemos ver, há uma implementação significativa já do DNSSEC. Isso deve ser considerado junto com os computadores quânticos, se, no caso, supomos que a validação vai aumentar no futuro, igual que as firmas que vemos aqui na esquerda, no quadro da esquerda.

Então, se queremos proteger o DNSSEC contra os computadores quânticos, temos que identificar essas três estratégias que vemos aqui. Por uma parte, que chamamos de substituição, a outra de

redesenho e outra de retirada. Substituir significa substituir os algoritmos criptografados que existem hoje para que alguns sejam seguros para esses computadores quânticos.

Redesenhar significa redesenhar o sistema do DNSSEC por completo, que é a segunda opção que aparece na tabela. E a terceira seria retirar. O que significa eliminar o DNSSEC por completo. E essas três abordagens têm vantagens e desvantagens. Por exemplo, a estratégia de substituição é relativamente fácil de implementar e de normalizar ou padronizar, mas tem alguns riscos operacionais. E depois vamos falar ao respeito de redesenho, e como começar do zero com o DNSSEC novas tecnologias como as árvores de Merkle, que reduzem os riscos, mas basicamente temos que renovar todo o sistema do DNSSEC e os seus protocolos, o que levaria muito tempo.

E depois a opção de retirada, o DNSSEC pareceria fácil, mas tem um impacto porque se eliminarmos o DNSSEC, abrimos o DNS a todo tipo de ataques, o DNSSEC tenta proteger o DNS de todos esses ataques. Então, no nosso trabalho, optamos mais pela primeira alternativa, que é a de substituição, por isso aparece aqui na cor verde. E vamos falar dessa abordagem daqui em diante.

Eu não vou explicar esse gráfico, tenho medo, mas o que vem aqui são as interações produzidas entre os resolutores e os servidores de nomes autoritativos, com as mensagens do DNSSEC que apresentamos aqui. E essas mensagens, na cor vermelha e

amarela, significa que tem já firmas, assinaturas ou senhas públicas, e esses têm que ser atualizados.

Seguinte slide. E para dar uma ideia de como aparecem essas firmas ou assinaturas, há dois exemplos aqui. Na parte de cima do slide, vemos uma senha pública, na esquerda, assinada. O que está sendo utilizado no DNSSEC, e na cor cinza, temos uma firma gerada por essa senha. E na cor azul clara, ou azul, vemos essa senha pública e a firma do DNSSEC, que é criada por um algoritmo pós-quântico, ou seja, é suficientemente forte como para proteger os computadores quânticos. E podem ver que é um pouco mais extensa. Isso é apenas para dar um indício, uma ideia, de como se veria de uma perspectiva técnica este tema. Seguinte, por favor.

Então, há diferentes algoritmos que são seguros perante os computadores quânticos, que se aplicam principalmente no contexto de NIST, que é o Instituto Nacional de Normas e Tecnologia dos Estados Unidos, que utilizou especialistas em criptografia para desenvolver um algoritmo que pode suportar o computador quântico. Então, aqui temos exemplos com alguns nomes curiosos, Falcon, SQSign.

E experimentamos com esses algoritmos e validamos o tempo que leva firmar ou assinar os seus próprios arquivos, por exemplo, a zona .nl, para poder validar os registros do DNS. E também temos os tamanhos de firmas e os tamanhos das senhas que podem diferir de grande forma. E o que podem ver na tabela é uma concessão recíproca que se faz, porque podemos ter tamanhos de

firmas menores e, se temos esse tipo de tamanhos pequenos, a velocidade da firma pode aumentar ou vice-versa.

Seguinte slide, por favor. Muito bem, aqui vemos a primeira experimentação feita para a zona .nl. Tentamos assinar, não tentamos, assinamos ou firmamos a zona com dois algoritmos pós-quânticos. Eu não vou entrar nos detalhes, mas vemos que leva o dobro de tempo assinar a zona com esses algoritmos PQC. Então, geralmente leva 10 minutos assinar a zona .nl e com esses PQC, com esses algoritmos, leva 20 minutos essa firma, o que não está mal, mas aqui vemos que esses resultados estão bem do ponto de vista operacional.

Esta é a nossa situação atual no SIDNLabs. Nós identificamos temas que gostaríamos de continuar estudando no futuro, que em grande medida tem a ver com o tamanho destas firmas e senhas públicas, e também queremos estudar o tempo de validação nos resolutores com maiores detalhes, junto com, por exemplo, o papel da memória rua, cachê-cachê.

Por último, tenho algumas sugestões para o GAC. Tenho algumas sugestões para o GAC. Talvez possam trabalhar com a agência dos Estados Unidos, que se ocupa desse tema, para ver como estão se alinhando com o algoritmo PQC que eles estão desenvolvendo. Eu sei que essa agência está interessada neste tema, em grande medida. Também podem incentivar o desenvolvimento de software de código aberto que integre os algoritmos PQC ao DNS e

a sua infraestrutura. Talvez isso possam fazer com fundos do NLNet ou Sovereign Tech Funds, Fundo Técnico Soberano.

Também talvez possam incentivar o desenvolvimento, desculpem, o desenvolvimento, sim, para a implementação do sistema, talvez com um site como talvez .nl, possam ver as propriedades no nome de domínio, e ali também, de forma rápida, possam incluir verificações para ver se os seus domínios estão prontos para a implementação do PQC.

E por último, quero também dizer que temos que continuar investigando o impacto operacional desses novos algoritmos PQC, se é que vamos seguir essa estratégia de substituição, e temos que ver as consequências, tanto nos operadores como na zona raiz. O software que desenvolvemos é utilizado para os nossos experimentos, utilizamos um software de teste de código aberto, aí está o código QR, podem descarregar esse software, e com todo prazer vou responder as suas perguntas.

MARCO HOGEWONING

Muito obrigado pela apresentação. Todos vamos poder descarregar, então, esse software quântico. Muito obrigado. Temos aqui algumas ações sugeridas, que são ações-chave, e da perspectiva governamental, no governo de Países Baixos, começamos a fazer gestão de ativos. O DNS está em toda parte, com o qual as DNSSEC estão em toda parte, e já estamos internamente trabalhando para ver onde precisamos tomar ações, fazer substituições, e posso dizer, por experiência, que isso leva

tempo. Agora, Peter está online e Barry na sala, querem tomar a palavra. Fala, Barry.

BARRY LEIBA Quero dizer uma coisa, esclarecer algo. Quando falamos em criptografia pós-quântica, devemos salientar que existe um conceito errado, conforme o qual os computadores quânticos colocam em risco tudo aquilo que for encriptado. Ele falava de assinatura, assinar, esse é um tipo, em particular, que está encriptado e que se coloca em risco a partir da quântica. Aquele outro que usamos, a internet, não está em risco, mas aquele encriptado que se usa para chaves e senhas.

CRISTIAN HESSELMAN Em geral, temos que ver casos de uso, requisitos específicos, então temos que ver quais são os casos de uso crítico que gostamos de estudar.

MARCO HOGEWONING Muito bem. Agora, Peter, está online.

PETER THOMASSEN Estou na sala, em realidade. Sou membro do SSAC. Quero falar sobre um aspecto. Há um baixo número de assinaturas em DNSSEC, mas se vemos os números abstratos, há mais de 10 milhões de nomes de domínio, e isso é significativo. Não sabemos qual é o método de assinatura quando se passa das DNSSEC para

a assinatura pós-quântica. Há mais de 10 milhões de domínios atualmente, talvez sejam mais, mas não poderemos fazer a transição se não é bem coordenada.

Então, isso é muito importante. No mapa que o senhor mostrou, vimos países de cor azul que têm ccTLDs que estão alinhados para fazer essas mudanças. Então, se seus países quiserem fazer essa transição automática no SSAC, vamos poder ajudá-los. Estão à disposição, bem como outros membros do SSAC.

MARCO HOGEWONING Muito obrigada. Temos algo de tempo ainda? Podemos pegar mais perguntas.

NICOLAS CABALLERO Muito obrigado. Obrigado por essa maravilhosa apresentação, Ram e equipe. Sempre um prazer recebê-los na nossa sala. Quero dizer duas coisas. Ram, Christian, queria saber se podemos aproveitar que está Jim Galvin aqui e quero saber se podemos aproveitar essa oportunidade para preparar uma apresentação para o board em Mascate para a reunião em Oman. Talvez devamos fazer uma versão um pouco mais leve da apresentação, porque há três ou quatro membros do board que têm um grande conhecimento técnico, mas os outros não.

Também quero dizer o seguinte, aproveitando que está aqui meu prezado colega do Brasil, estamos organizando uma sessão regional de criação de capacidades para países latino-americanos,

que será em Brasília ou São Paulo. Temos que decidi-lo. Bom, antes ou depois da reunião de Oman, poderiam nos ajudar a preparar esse evento? Queremos falar da implementação das DNSSEC, queremos falar em criptografia simétrica e assimétrica e queremos ver, por exemplo, o que está acontecendo, me corrijam se eu me engano, mas faz duas ou três semanas o RSA ficou sem efeito, se quebrou. Não sei se isso foi assim ou não.

De qualquer forma, há muitas vantagens o software de código aberto para os governos. Eu sou um grande usuário desse tipo de software gratuito e de código aberto, mas é difícil explicar de forma simples aquele que não tem um conhecimento técnico, explicar quais as vantagens, não só técnicas, mas também econômicas e todas as vantagens que oferece todo esse tipo de licenças.

Então, talvez com a ajuda de vocês, com o seu conhecimento técnico, poderíamos ter mais um pouco de sucesso. Então, dois pedidos para resumir. Ajudar-nos a preparar uma apresentação para o board e ajudar-nos a preparar o evento regional de criação de capacidades para a América do Sul, para os países dessa reunião, que talvez esse evento seja feito em Brasília ou em São Paulo.

RAM MOHAN Muito obrigado, Nico, por esse pedido. Realmente estamos muito empolgados, queremos colaborar e fico à disposição e vamos conversar ao respeito.

CRISTIAN HESSELMAN O mesmo da minha parte.

NICOLAS CABALLERO Podia dizer alguma coisa sobre o RSA?

WARREN KUMARI Acho que você fala sobre um documento acadêmico publicado pela Google, que diz que agora é mais fácil evitar o RSA. Os níveis necessários já são menos exigentes, que há menos complexidade nos computadores quânticos necessários há uma menor quantidade de bits quânticos para ter um sistema confiável.

E no documento se diz que justamente não são necessários tantos bits como se pensava, mas não fica claro até que grau temos que nos preocupar daqui para o futuro, ou seja, o RSA ainda funciona. O que acontece é que daqui a uns anos, aparentemente, sim, é provável que deixe de funcionar, mas as estimativas não são totalmente exatas. Basicamente, se pega uma média de estimativas formuladas por cientistas que se encarregam do tema quântico. Pode ser amanhã, ou daqui a 50 anos, ou a 500 anos, é difícil predizer.

Obviamente, existe uma grande possibilidade de que seja daqui a alguns anos, mas é como a energia da fusão do átomo. O que se passou não se soube quando ia estar pronta essa tecnologia até que aconteceu. Bom, podemos falar do RSA ou de outros sistemas

	criptográficos que estão vulneráveis. Então, temos que estar nos preparando para o futuro.
NICOLAS CABALLERO	Quer dizer que temos que consertar a goteira quando ainda não está chovendo. Perfeito.
MARCO HOGEWONING	Bom, temos um pedido da palavra de Austrália.
INGRAM NIBLOCK	Quero ver uma tabela onde se vê uma comparação entre o tamanho das senhas. Entendo o tema do tamanho dos pacotes UDP. Qual seria o efeito prático de ter tempos de assinatura mais extensos? Por exemplo, para .nl, uma diferença de 2 a 10 minutos. Isso é problemático se deve ser feito de forma reiterada? Esse é um problema no DNS?
CRISTIAN HESSELMAN	Temos 6,2 milhões de domínios na nossa zona e a publicação é de 30 minutos aproximadamente. Quer dizer que a cada 30 minutos tem que voltar a assinar. Então, se o tempo de assinatura leva muito tempo, acaba o tempo para publicar. É isso que devemos considerar. Isso tem a ver com o modelo de implementação. O Christian tem um modelo de zona completa, mas há um outro modelo de assinaturas em tempo real para cada consulta. É difícil

dar uma resposta em geral, mas, sim, a velocidade é um fator importante.

GREG Talvez, quanto mais demorar em assinar, talvez tenha que fazer mais modificações no modelo que se utiliza.

MARCO HOGEWONING Bom, muito bem. Obrigado. Espero que sejam respondidas as perguntas. Depois vamos fazer a pausa para o café. Podem ter diálogo, comentário com os colegas nessa pausa. Quero agradecer a todos os painelistas que se uniram nessa sessão por essa informação de tanta utilidade e por nos ajudarmos a entender todos esses conceitos técnicos. Antes da pausa para o café, quero dizer que temos que voltar à sala do GAC para a sessão sobre WHOIS e exatidão dos dados. Espero que tenham desfrutado dessa sessão e aprendido. Desfrutem do café. Muito obrigado.

[FIM DA TRANSCRIÇÃO]