ICANN79 | Fórum da Comunidade – Conheça a comunidade da ICANN: evento de integração do membros do SSAC e RSSAC
Domingo, 3 de março de 2024 – 4h30 às 5h30 SJU

SIRANUSH VARDANYAN: Muito obrigada. Estamos na nossa última sessão de hoje com colegas e membros da próxima geração para falar sobre o aspecto de segurança e estabilidade da ICANN, e é um grande prazer que tenho o presidente do RSSAC, que é o Comitê Consultivo do Sistema de Servidores Raiz e do SSAC, que é o Comitê Consultivo de Estabilidade e Segurança. Eles vieram até nós e temos o prazer de conversar com eles neste ambiente, quase cara a cara. Teremos 30 minutos para o início do RSSAC, depois 30 minutos para o SSAC, e depois 5 a 10 minutos de apresentações e depois perguntas e respostas. Ram, por favor, venha se juntar a nós. Portanto, o primeiro apresentador será o Presidente do RSSAC, Jeff, que é o Presidente do RSSAC e ele estará falando e explicando o que esta comunidade está fazendo e quão importante você é, e também como os recém-chegados podem se envolver. Muito obrigado. A palavra é sua, Jeff.

JEFF OSBORN: Olá. Você pode me ouvir? Esta é a primeira parte da interação com o público. Essa foi a mais fácil. Fica mais difícil. Meu nome é Jeff Osborn. Sou o presidente do RSSAC, que é a organização da ICANN que presta consultoria em questões relacionadas ao sistema de servidores raiz

DNS. E fomos incumbidos de tentar explicar o que fazemos de uma forma mais simples. E então ouvi dizer que precisava falar com vocês. Então, passamos muito tempo montando esta apresentação para tentar explicar às pessoas que não usam DNS o dia todo o que é DNS e como funciona o sistema raiz. Então, no final disso, vocês serão especialistas. Você terá uma nova página em seu currículo. Você provavelmente conseguirá empregos muito melhores imediatamente, provavelmente amanhã. Mas você terá que prestar atenção porque é um pouco complicado. Então, hoje estamos trabalhando em um slide de três dias. Há algumas pequenas coisas aqui que vou abordar porque, como eu disse, esta é a primeira vez. Aprenderemos aqui como o DNS funciona, qual é a função do sistema de servidor raiz no DNS e aprenderemos sobre a importância do sistema de servidor raiz. O Comitê Consultivo do Servidor Raiz é composto pelas pessoas que operam os servidores raiz. Existem 12 organizações que operam os servidores raiz. Há um membro e depois um membro suplente, então são duas vezes 12, ou seja, vocês são bons nisso. Você conseguirá esses empregos. 24, e temos contatos com algumas outras organizações, como o Conselho da ICANN, ou, se você já ouviu falar, a Força-Tarefa de Engenharia da Internet, o Conselho de Arquitetura da Internet, várias organizações técnicas por aí. Portanto, tentamos obter conhecimento especializado de onde pudermos, e aqui está o que fazemos. Então deixe-me apresentar a você o DNS. Agora, ICANN, uma das primeiras coisas que notei sobre ICANN é por que não se escreve apenas ICANN. Seria pronunciado da mesma forma. Existem dois Ns na ICANN por um motivo. Isso porque um N são nomes e um N são números. Portanto, se

você estivesse tentando lembrar uma longa sequência de números, teria mais dificuldade do que se estivesse tentando lembrar uma palavra. Portanto, o DNS usa nomes humanos para encontrar endereços de computadores. Os próprios computadores não têm ideia do que é amazon.com. O que eles entendem é uma sequência de letras. Portanto, os humanos conhecem um nome de domínio, amazon.com. Eu gostaria de ir para lá. O computador espera ouvir 18.239.62.181, que é literalmente o endereço IP da Amazon hoje. Então o DNS traduz isso. Você digita em um navegador. Ele é traduzido pelo sistema DNS e, na maioria das vezes, você pode usar o mesmo nome, independentemente do que esteja mudando em segundo plano. Os números podem ir para lugares diferentes, países diferentes, servidores diferentes, mas você sempre usa apenas um nome. É um sistema muito conveniente e, em sua raiz básica, está o sistema de nomes de domínio. Então, quando as pessoas falam sobre o DNS, trata-se de usar palavras para chegar aos números. Alguém precisa que eu repita isso ou isso faz sentido? Palavras para encontrar números. Excelente.

SIRANUSH VARDANYAN: Polegar para cima.

JEFF OSBORN: Perfeito. Bom. Portanto, a maioria dos dispositivos conectados usa o DNS para acessar qualquer coisa na Internet, e a Internet, você deve ter ouvido falar, é grande. Então é difícil e é assim que fazemos. Obviamente, existem coisas como computadores e servidores que usam isso para se conectar, mas cada vez mais os telefones celulares

são provavelmente um usuário maior, e Deus me livre, parece máquinas de lavar, geladeiras, campainhas e todo mundo por aí. Todos nós usamos o DNS para nos orientar na Internet. Os benefícios deste sistema são que você só precisa lembrar o nome. Se o seu computador quebrar e você adquirir um novo, ele ainda poderá ser chamado de Jeff'sComputerHut.com. Não importa se meu servidor mudou, eu mudei de rua ou meu prédio pegou fogo. Então você tem portabilidade de serviço. Isso é algo muito importante em termos de não ficar preso a um fornecedor. Você não fica preso a um ISP. Você nem fica preso em um país. É como as pessoas que têm um nome de domínio, agora aqui está outra coisa dentro da ICANN. Você não é proprietário de um nome de domínio se tiver um nome de domínio. Você é um registrante. Então, quem aqui é registrante e não sabia que era registrante? Isso é outra coisa para colocar no seu currículo. Você pode colocar, eu sou um registrante real. Garanto que são mais 10% de salário na maioria dos lugares. É um segredo pouco conhecido, dica profissional. O principal benefício do DNS no final das contas é que ele é um identificador fácil para humanos. É mais fácil saber que sou jeff@isc.org do que jeff@118.36.12.92. E posso literalmente lembrar que houve um dia em que você teve que fazer esse tipo de bobagem. Portanto, este é um sistema melhor.

SIRANUSH VARDANYAN: Jeff, se eu puder pedir para nossos intérpretes desacelerarem, seria ótimo. Obrigado.

JEFF OSBORN: Existe um antídoto para o café? Vou tentar desacelerar.

SIRANUSH VARDANYAN: Obrigado.

JEFF OSBORN: Isso é difícil. Gosto de falar rápido. Vou tentar desacelerar. Os dispositivos obtêm esses endereços de algo que você chama de resolvedor. Você provavelmente já ouviu o termo resolvedor por aqui. Existem milhões deles em todo o mundo. O mais familiar para você pode ser 8.8.8.8, um resolvedor que o Google colocou em todos os lugares. E se você apontar sua máquina para ele, ele lhe dirá onde estão as coisas. Existem milhões e milhões dessas coisas por aí. E eles basicamente agem como se pudessem ler listas telefônicas. Portanto, a ideia é que a lista telefônica seja algo chamado de servidor autoritativo, e os números nela contidos sejam dados de zona. E quando você perguntar, ei, onde fica www.amazon.com, eles podem procurar aqui, e aí está o endereço. Isso acontece em milissegundos. É incrivelmente rápido e acontece um número impressionante de vezes. Estimamos que, num dia médio, isso aconteça 500 trilhões de vezes. 500 trilhões é muito. Se você começasse agora e contasse até 500 trilhões, nunca terminaria. É um número grande. Os próprios resolvedores obtêm seus endereços de algo chamado servidor autoritativo. Então, vamos começar agora com o processo de como essas coisas realmente se conectam na rede, quem fala com quem e de onde vem tudo isso. Os resolvedores são questionados o tempo todo: como faço para chegar à Amazon? Bom, na memória eles guardam o

endereço, porque você não quer ter que procurá-lo toda vez. Então, se você fizer perguntas simples como onde está amazon.com, onde está o tinder.com, onde estão essas coisas, eles podem simplesmente entregá-las a você sem memória. Isso é chamado de cache. Eles armazenam isso em uma coisa chamada cache. É daí que vem a maioria das respostas. Quando você pede informações sobre como encontrar algo em mais de 90% das vezes, é daí que vem, da memória. De vez em quando, você precisa obter um novo número ou confirmar um antigo e ele precisa ir até um servidor e procurá-lo. Atenção, aqui está a parte técnica. Há um processo de três níveis pelo qual ele deve passar. Dependendo de quanta informação você precisa saber sobre esse endereço, você irá perguntar ao servidor autoritativo de nomes de domínio ou ao servidor autoritativo de nomes de domínio e ao servidor de domínio de nível superior. O domínio de nível superior é o mesmo que o.com, o. Reino Unido, o. nl, tanto faz. Ou o servidor de nomes de domínio, o servidor de domínio de nível superior e um servidor raiz, dependendo do quanto o seu computador não sabe. Então, vamos orientá-lo no gráfico. Este gráfico é a melhor coisa para aprender como isso funciona ou é tão confuso que você vai me dizer por que colocou todas aquelas letras ali? Eu não consigo ver isso. Então trabalhe comigo. Vamos tentar descobrir isso. Na primeira passagem, isso está lá em cima. Você consegue ler essas cartas? Bom. Na primeira passagem, a caixa cinza é o resolvedor e estamos fazendo uma pergunta. Estamos começando de fora e dizendo: ei, estou tentando chegar ao endereço www.amazon.com. Eu sei onde está? Clique. E o resolvedor diz, sim, eu aceito. Está na minha memória. Então aqui está.

Aqui está o endereço. E assim voltamos ao fim. E à direita você pode ver onde diz aqui está a rotina. Isso é mais de 90 em 100 vezes. Isso ocorre em mais de 90% das vezes, você apenas obtém isso da memória. Mas existem centenas e centenas de milhões de endereços por aí, então às vezes você não os conhece. E daí se eu não souber a resposta? A primeira pergunta que você faz é: sei onde está o servidor que pode saber a resposta? E se fizer isso, você manda a pergunta, ei, preciso saber o endereço IP de www.example.com. Acabamos com um servidor oficial porque example.com tem seu próprio local para procurar todas as letras. O que vem na frente de example.com? Poderia ser www. Pode ser correio. Pode ser uma série de coisas. A gente pergunta e ele volta e vai, aqui está o endereço. Nós nos lembramos disso e agora perguntamos: já sabemos a resposta? Sim nós fazemos. Então, examinamos os dois casos simples. Já sei a resposta? Sim, está na memória. Ou já sei a resposta? Não, mas sei onde está o servidor que sabe a resposta. Isso me diz, agora guardo isso na memória e já contei. A única coisa que torna isso complicado é que são centenas e centenas de milhões de dispositivos, então eles não podem viver todos em uma máquina, então ela tem três camadas inteiras. Então, se você não tem como chegar a example.com, você precisa dar um passo adiante e ir, bem, que tal não www.example.com, mas example.com? Esse servidor é separado. É chamado de servidor TLD. Se você obtiver a informação disso, ele voltará e dirá: sabemos onde fica. Sabemos onde estamos agora? Não, você acabou de descobrir onde está example.com. Temos que voltar e adicionar www e agora conhecemos ambos. Este é um circuito que vai descer três degraus e quando você chegar ao terceiro

degrau, estará pronto. Então, se você descobrir isso e seguir em frente, é assim que o DNS funciona. Se você não sabe absolutamente nada, se o seu computador acabou de sair da caixa, ele não tem memória e não sabe de nada, ele sabe de uma coisa. No canto inferior esquerdo, ele conhece os endereços dos servidores raiz. Somos nós. Existem 12 endereços para os 12 operadores de servidor raiz e você pode encontrar um deles e dizer: ei, onde está a lista de.com? Eu não sei de nada. Eu só preciso saber quais são as coisas à direita do ponto? Estou procurando o.com e depois vou perguntar onde está o exemplo e depois vou perguntar onde está o www. Você obtém essa resposta, guarda na memória, volta e procura por exemplo, volta e procura www. Você construiu o nome encontrando todos os endereços. Você o tem em seu armazenamento. É isso. Agora vocês são todos especialistas em DNS. Isso vai para o seu currículo. Parabéns. Você pode deixar sua mensalidade na porta. Aceitamos dinheiro, gorjetas. O interessante disso é a frequência. Se você vir as letras vermelhas ao lado, o número de vezes que isso acontece sem memória é superior a 90%. O número de vezes que você tem que descer e dizer, ah, droga, eu nem sei o que é example.com, é cerca de outros 5%. Ter que sair e dizer onde está.com e o que ele sabe? É cerca de 2%. Ir até a raiz, até o servidor raiz, é cerca de uma em 5.000 tentativas. Somos muito importantes se você esquecer tudo, mas não é como se toda vez que você sai e faz alguma coisa, você tenha que acessar um servidor raiz. Nós somos seu backup. Isso faz sentido? Isso deveria ser uma camiseta? Eu estava pensando sobre isso. Pode ser muito difícil de ler. Tenho outro slide de camiseta chegando, então vamos descobrir isso. De qualquer forma, em análise,

o servidor raiz mantém uma cópia dos dados da zona raiz, e a zona raiz informa o que os TLDs possuem. Você só quer saber, me conte tudo que termina em.com. Conte-me tudo que termina em. Reino Unido. Conte-me tudo que termina em. nl e lhe dará tudo isso. Isso lhe dará a única palavra à esquerda. O servidor autoritativo do TLD, o segundo degrau abaixo, conhece todos os endereços para o próximo passo. Uma vez que você tenha Amazon e.com, ele conhece www, e conhece mail, e conhece servidor de nomes, e conhece retornos, e conhece John ponto tanto faz. Qualquer outra coisa desse lado. O resolvedor é o dispositivo que vai lá e sabe como empilhar esses três processos e obter as informações necessárias para que você tenha o endereço de onde está tentando ir. No mundo de milissegundos em que isso acontece, as consultas aos servidores raiz são realmente raras. Nós nos deparamos com isso o tempo todo, porque o servidor raiz é absolutamente necessário se você esquecer tudo, as pessoas pensam que é absolutamente necessário em cada etapa do caminho, e isso não é verdade. É algo muito importante de se ter, mas no grande esquema das coisas, você nem sempre opera através do servidor raiz. Cada vez que sua avó pesquisa como fazer biscoitos açucarados, o servidor raiz não está envolvido. É envolvido muito raramente, e tenho algumas pessoas que argumentam que é uma em cada 10.000 vezes. É pelo menos um em 5.000. Simplesmente não é algo que acontece muito. Isso faz sentido? Este é o slide que tiramos esta manhã porque Ram gostou e acidentalmente o colocamos de volta, então é meio engraçado. Vou ter problemas por mostrar esses números porque disseram que não dá para provar, mas temos certeza de que está certo. É discutível que o

número de pesquisas que acontecem, essas solicitações, num dia seja de cerca de 500 trilhões com um T. É um número chocante. É um número inacreditavelmente alto, mas você pensa em todas as vezes que tem uma URL em seu computador e precisa descobrir alguma coisa, e todo mundo faz isso. Isso é sobre o número. Acreditamos que os servidores raiz recebem cerca de 100 bilhões de perguntas por dia, o que ainda é um número enorme, mas é apenas cerca de uma em 5.000 do número total. Então, estamos falando de números muito grandes, e é isso que fazemos. É importante lembrar que embora o volume seja grande, a frequência não. O que fazemos para garantir que esse recurso valioso sempre funcione? Um par de coisas. Primeiro, é extremamente redundante. Cada servidor raiz contém todas as informações. Se você acessar algo como.com, precisará lembrar 140 milhões de coisas para colocar à esquerda de.com. Os servidores raiz só precisam lembrar os 1.700 TLDs. Existem apenas 1.700 palavras atualmente à direita do ponto, de.com a. edu para NL para todos os códigos de países, todos os códigos comerciais. 1.700 deles. No texto, essa não é uma informação muito grande. Acontece que cada um desses servidores raiz por si só poderia lidar com a maior parte da demanda terrestre. Temos 1.700 deles. Quando você tem dois computadores com dupla finalidade para backup e um deles morre, o outro ainda funciona. Temos, no mês passado, acho que eram 1.758 deles em todo o mundo, e 1.757 deles nem são realmente necessários. Você poderia imaginar uma situação em que perdeu tantos e tudo ainda funciona. Este é um sistema chocantemente resiliente. Temos diversas plataformas de hardware. Todo mundo usa computadores diferentes para executar as coisas.

Usamos diferentes sistemas operacionais. Todo mundo usa diferentes. Usamos diferentes aplicativos DNS. No meu trabalho diário, sou presidente de uma empresa chamada ISC e, além de operar o servidor F-Root, desenvolvemos e mantemos um software chamado By9, que nas últimas três décadas e meia tem sido um dos principais peças de software DNS. Mas muitas outras pessoas não o usam. Eu vi Andre aqui. Existem fabricantes de outros, não, ele não está aqui. Existem fabricantes de outros softwares que funcionam o tempo todo. O que é ótimo é que se todos os computadores Dell funcionassem, o servidor raiz ainda funcionaria porque todos nós usamos coisas diferentes. Se um sistema operacional entrar em colapso, se o Windows morrer amanhã, estaremos executando vários sabores de Unix. Se By9 morresse amanhã, teríamos todos os tipos de outras aplicações. É um sistema surpreendentemente diversificado e resiliente, sem nenhum ponto único de falha técnica. Além disso, não há nenhum ponto de falha institucional, onde você se preocupa, bem, e se esta empresa tiver um problema e tiver um processo judicial? E se alguém te processar? E se alguém disser que você não presta mais? E se você ficar sem dinheiro? Não importa. Somos 12 organizações separadas. Nós passamos muito tempo juntos. Provavelmente vejo algumas dessas pessoas com mais frequência do que vejo meus filhos, mas meus filhos são adultos, então não é tão ruim assim. Cooperamos, mas estamos todos separados. Somos organizações separadas, portanto um ato que prejudique uma organização não irá prejudicar todo o nosso grupo. Não há um único ponto de falha institucional. Agora, além disso, este é um pouco difícil para quem é novo nisso, mas há um boato

generalizado de que nós, os operadores de ganhos de raiz, podemos controlar os dados do que você vê. Podemos controlar quem você pode chegar e onde você pode chegar. Não poderia estar mais longe da verdade. Se você tiver um domínio, poderá dizer aonde ele se conecta e passá-lo para o seu registrador, que o repassará para um grupo chamado IANA. A IANA coloca tudo em um pacote, e aquele cara ali está envolvido com uma organização chamada, ele não está olhando. Ele está envolvido com uma organização chamada Root Zone Maintenanceer. Eles o embalam criptograficamente, por isso é absolutamente seguro. Passe-o para nós e nós o distribuiremos para todos os 1.758 ou quantos forem agora. Servidores raiz em todo o mundo, e todos vocês têm essas informações. Nós não mudamos isso. Nós não abordamos isso. Nós não ajustamos isso. Nós não editamos. Pegamos as informações que chegam até nós e as servimos ao mundo. Há 40 anos fazemos isso. Isto está operando há 40 anos este ano sem falhas. O sistema não caiu sistematicamente de forma alguma em 40 anos literais. Se você conhece computadores, percebe que esse é um número incrível. Também é interessante se você quiser realmente entrar em um buraco de rato, o sistema de endereçamento que usamos é chamado Anycast e meio que impede o funcionamento do DDoS. Você simplesmente não pode fazer DDoS na instância Anycast de uma forma que possa derrubar coisas normais. Não estamos pedindo às pessoas que tentem, mas muitas pessoas tentaram, e o sistema simplesmente não caiu. Então, em resumo, o sistema do servidor raiz é realmente importante, embora pouco frequente, parte da resolução de endereços que é usada muitas, muitas, muitas vezes hoje por praticamente todos

os usuários da Internet no planeta. A maioria das consultas sai da memória e a maior parte delas nunca chega a um servidor raiz. Os operadores do servidor raiz não controlam o conteúdo. O sistema é notavelmente forte, resiliente, diversificado e simplesmente funciona, e é assim que funciona o sistema de servidor raiz. Muito obrigado.

SIRANUSH VARDANYAN: Isso é muito impressionante, Jeff, muito. Você tem mais um especialista em DNS sentado ao seu lado. Muito obrigado.

JEFF OSBORN: Coloque no seu currículo e peça um aumento.

SIRANUSH VARDANYAN: Muito obrigado. É realmente muito interessante. Alguma pergunta? Sim por favor. Filomeno, você usa o microfone ali. Portanto, temos cerca de sete minutos para perguntas a Jeff e depois passaremos para o SSAC.

ZOE FILOMENO: Olá, meu nome é Zoe Filomeno, bolsista do ICANN79. Venho de uma formação interdisciplinar de tecnologia restrita, interfaces cérebro-computador para pacientes com doenças degenerativas.

JEFF OSBORN: Você consegue se aproximar do microfone?

ZOÉ FILOMENO: Sim. Perfeito.

JEFF OSBORN: Dá pra ouvir muito melhor.

ZOE FILOMENO: Então, interseccionalidade de tecnologia estreita, interfaces cérebro-computador e tecnologias emergentes. A minha pergunta é em relação às tecnologias emergentes e como muitos dos sistemas parecem seguir a ligação humana dentro do sistema da nossa própria criação. Então, basicamente, o que estou afirmando é que tudo que existe neste sistema é o nosso próprio sistema nervoso. Só me dê um segundo. Então o sistema nervoso, a memória, a forma como acessamos é como os servidores raiz acessam. Portanto, em implicações futuras, minha preocupação é com pacientes que possuem interfaces cérebro-computador que possam estar conectadas à Internet. Haveria um futuro onde você, Jeff ou qualquer pessoa lidaria com a política disso e como tudo isso está funcionando? Espero que faça sentido. Desculpe.

JEFF OSBORN: Essa é a melhor pergunta que já recebi na ICANN. Posso não ser inteligente o suficiente para responder adequadamente. Santa cavala.

ZOÉ FILOMENO: Sim. Na verdade, a IANA já me disse que não vão lidar com o problema a menos que se torne um problema atual.

JEFF OSBORN: Isso é basicamente o que, infelizmente, eu teria a dizer. É muito, muito interessante tentar olhar para o futuro e ver o que acontece. E estou envolvido com a internet há mais tempo do que gostaria de admitir. E errei muitas vezes ao adivinhar o que iria acontecer. Nunca vi a mídia social chegando. Isso foi um choque completo. Então, eu provavelmente acho que estou errado sobre isso. O que estamos fazendo é muito divertido é que basicamente a maioria das pessoas com quem trabalho mantém essa coisa de internet funcionando. E estamos entusiasmados com o que as pessoas fazem com isso. O que fazemos é tentar mantê-lo confiável. Tentamos mantê-lo rápido. Tentamos mantê-lo disponível para o maior número possível de pessoas no planeta, funcionando da melhor forma possível. E então sentamos e observamos pessoas como você fazendo coisas incríveis com isso e pensamos, oh meu Deus, nós fizemos parte disso. Então, estarei observando o que você faz, mas não sei o quanto farei além de tentar garantir que esteja sempre lá e disponível para você e rápido.

ZOÉ FILOMENO: Sim. E se eu puder acrescentar uma das principais situações quando você falou sobre ataques DDS, sou especialista na área de como os algoritmos matemáticos dentro da música afetam os neuroquímicos. Então, isso pode ser usado basicamente para se infiltrar ou hackear um humano, a fim de criar certas situações. Se isso for verdade no modo

como vocês operam, isso possivelmente significaria que, se vocês não tiverem problemas com os ataques DDS, isso pode ser verdade para pacientes com implantes. Então eu estou meio...

JEFF OSBORN: Os paralelos são interessantes. Tenho um filho que está tentando cursar medicina. Tenho discussões nesse sentido e isso é realmente difícil de fazer na frente de uma centena de pessoas, mas é uma pergunta muito interessante. Se você me encontrar no corredor, comprarei um café para você e poderemos conversar sobre isso. É muito interessante.

ZOÉ FILOMENO: Obrigada.

JEFF OSBORN: Claro. Obrigado.

SIRANUSH VARDANYAN: Shanelle, por favor, vá em frente.

SHANELLE MCPHERSON: Sim. Boa tarde a todos. Meu nome é Shanelle McPherson, sou seguidora do ICANN79 e falo em minha própria capacidade. Em primeiro lugar, todos acabamos de nos formar com louvor. Obrigado, senhor. Isso é o primeiro. Minha pergunta é, e estou apenas curioso. Minha pergunta é para os novos gTLDs que estão prestes a sair, quero saber se eles já

estão incorporados no servidor ou é um caso em que são criados a partir da raiz, então se um novo gTLD for lançado, como funciona o servidor sabe que já está lá? É criado dentro da raiz? Essa é a minha pergunta.

JEFF OSBORN: Essa é uma excelente pergunta.

SHANELLE MCPHERSON: Sim. Obrigado.

JEFF OSBORN: A zona raiz é basicamente uma lista de todos os TLDs e, em seguida, um endereço para eles, na verdade um em IPv4, que é a versão de endereçamento que eu estava usando aqui, e também um IPv6 em geral, que é o mais longo, forma de endereçamento mais recente. Geralmente, cerca de duas vezes por dia, um novo arquivo de zona raiz é gerado. Então, quando eles surgirem com os novos TLDs, eles serão literalmente adicionados à lista e pronto. Assim que é gerado, duas vezes por dia, ele se apaga. Eles podem enviar mais. Alguém estava me dizendo outro dia que eles fizeram cinco empurrões em vez de dois. É muito rápido e tudo se tornará parte da zona raiz. Boa pergunta.

ORADOR DESCONHECIDO: Minha pergunta é: que tipo de técnicas e sistemas no sistema de servidor raiz do ponto de vista de proteção e monitoramento, para a verificação de integridade e para o desempenho de todos os sistemas

de servidor raiz, eu sei que existe um proteção em caso de falha, mas quais são os sistemas utilizados do ponto de vista de desempenho?

JEFF OSBORN: Uma das coisas interessantes sobre o servidor raiz e por que tentamos lembrar às pessoas como ele é usado com pouca frequência é que ele não faz parte da latência que as pessoas notarão em um dia normal. Se você pensar na última vez que pesquisou algo e inseriu um URL. Imagine quanto tempo você levaria para chegar à 5.000ª vez que fez isso. Suponhamos que um servidor raiz mais próximo de você tenha falhado. O próximo provavelmente estará a alguns milissegundos de distância. Na 5.000ª vez que você pesquisou algo, há 5 milissegundos adicionais no tempo de pesquisa. Quais são as chances de você notar isso? É literalmente usado com tão pouca frequência e é algo que, uma vez usado uma vez, acaba sendo colocado no cache, por isso tivemos muita dificuldade em tentar entender como um usuário final poderia notar não apenas um servidor raiz lento, mas também um servidor raiz com falha. um. Porque há muitos deles. Quando eu disse que os ataques DDoS não funcionam bem, usamos uma coisa muito interessante chamada Anycast. Imagine que você tivesse um restaurante com 1.000 garçons, todos chamados José. Se você levantar a cabeça e falar, ei, José, sempre tem um garçom lá. Se ele for para a cozinha, não importa se você falar José porque tem outro. Porque todas as instâncias do servidor F-Root ao redor do mundo, há quase 300 delas da minha empresa, estão todas com o mesmo endereço, então quando você diz, ei, servidor F-Root, não importa se este é morto. Há outro a 80 quilômetros além e 80 quilômetros além e 80 quilômetros

além. Do jeito que a internet funciona, ela continuará funcionando até encontrar aquela que funciona. Literalmente, o tempo adicional envolvido é de milissegundos. Fazemos muitas coisas de forma independente e cada organização tem maneiras diferentes de garantir que tudo esteja em ordem. Temos muito orgulho de como fazemos as coisas, mas todos nós as fazemos de maneira diferente por design, porque o que você não quer é ter uma monocultura onde uma única falha, um único bug ou um único problema derruba mais de uma coisa. Isso faz sentido?

ORADOR DESCONHECIDO: Claro. Obrigado.

JEFF OSBORN: Bom. Obrigado pela ajuda.

SIRANUSH VARDANYAN: Pessoal, não temos tempo para mais perguntas por enquanto porque precisamos ir para a apresentação do SSAC. Quer esperar até o final da sessão se tivermos tempo para mais perguntas e se Jeff ficará aqui?

OLORUNDARE JAMES KUNLE: Então, depois de mim ou…?

SIRANUSH VARDANYAN: Não, você também está incluído, mas se tiver 30 segundos para terminar, faça-o.

OLORUNDARE JAMES KUNLE: Ah, com certeza. Bom. Então meu nome é Kunle.

SIRANUSH VARDANYAN: Garantirei que nossa próxima geração seja a primeira a fazer a pergunta.

OLORUNDARE JAMES KUNLE: A questão é esta. Sinto muito, talvez eu tenha perdido quando fui para Eastman, é sobre quem pode ingressar no RSSAC e quem não pode, e quais são as condições para ingressar? Obrigado.

JEFF OSBORN: O RSSAC é composto por dois representantes de cada uma das 12 organizações que o atendem, e há também uma convenção política do RSSAC, composta por especialistas em DNS de todo o mundo. Para ser membro do RSSAC, você precisa operar uma das letras do servidor raiz. Para ser membro da convenção política do RSSAC, sou também o presidente do comitê de adesão da convenção política do RSSAC. Basta demonstrar conhecimento prático de DNS, pois não estamos fazendo treinamento. Estamos reunindo um grupo de especialistas que fazem a maior parte do trabalho. A maior parte do trabalho realizado pelo RSSAC é realizado pelo caucus, e este é um grupo diversificado de pessoas de todo o mundo. Há um monte deles aqui. Eu começaria a procurar, mas as luzes estão nos meus olhos. Tudo que você precisa fazer é ter um bom conhecimento prático de DNS e se inscrever. Isso

literalmente chegará a mim e a seis outros caras que analisarão e determinarão. Se você não for habilidoso o suficiente, recomendamos: ei, mostre-nos onde você acha que é habilidoso. Se isso não funcionar, podemos torná-lo um membro exclusivo da lista de e-mails, e você poderá servir até sentir que, ei, aprendi o suficiente e agora sei como fazê-lo. É um grupo muito inclusivo. Nós realmente procuramos muita ajuda, mas não é uma organização de treinamento. Precisamos de especialistas quando eles chegam lá, porque é assim que a maior parte do trabalho é feita. Isso ajuda?

SIRANUSH VARDANYAN: Obrigado, Jeff Osborn, presidente do RSSAC. Muito obrigado. Seus aplausos são para Jeff, mas Jeff, por favor, fique conosco. E é com grande prazer que apresento agora o presidente e vice-presidente do SSAC, Ram Mohan e Tara Whalen. Ram, é tão bom ver você vindo para o programa de bolsas. Quando eu era bolsista, era você quem fazia a apresentação para a comunidade e eu gostava muito, então obrigado por ter vindo. O chão é seu.

RAM MOHAN: Muito obrigado. E uma boa noite para todos vocês aqui. É realmente um prazer estar aqui. Obrigado por convidar Tara e eu aqui. Então, antes de entrar na apresentação, quero contar uma história. E esta é a história do SSAC. Desde a década de 1990, antes de muitos de vocês nascerem, mas desde a década de 1990, tem havido preocupações sobre ataques a infraestruturas críticas da Internet, ataques terroristas a infraestruturas críticas da Internet. Esta é uma preocupação há muito

tempo. E as pessoas reunidas falavam sobre isso e depois se dispersavam. Eles diriam, bem, isso é importante. Talvez devêssemos acompanhar isso, deveríamos continuar. E então, em 2001, aconteceu o 911. E isso foi um ataque concertado, não à infraestrutura da Internet, mas a outros tipos de infraestrutura, outras coisas que aconteceram. E realmente aumentou a consciência global de que se os terroristas, além das coisas que fizeram, também tivessem atacado infraestruturas críticas da Internet ao mesmo tempo, teria sido uma ampliação ainda maior da perturbação e dos problemas que aconteceram então.. Então, depois de setembro de 2001, em novembro de 2001, a ICANN se reuniu em Marina del Rey, na Califórnia, nos EUA. E nessa reunião, algumas das pessoas que estavam na ICANN, algumas das pessoas que também estavam ajudando a coordenar algumas das reuniões gerais respostas governamentais aos ataques terroristas, uniram-se e retiraram alguns de nós que operávamos directamente infraestruturas críticas. Naquela época, minha empresa, e eu era o CTO dessa empresa, operava o domínio de nível superior.info, que era um domínio novo, mas ainda era uma parte significativa dele. Havia pessoal da VeriSign que operava não apenas os servidores raiz, mas também operava.com,.net e.org naquela época. Algumas outras pessoas que operavam códigos de país nos reuniram e disseram: vocês podem começar a pensar sobre o que pode acontecer se houver um ataque e se seus domínios forem assumidos ou retirados? Porque até então, enquanto havia um certo desconforto, havia essa ideia, vai ficar tudo bem. Somos todos boas pessoas trabalhando de boa fé e tudo vai ficar bem. Construa defesas decentes, construa sistemas decentes, mas você não precisa

necessariamente se preocupar muito mais. Em 2001, dentro da ICANN, criamos um novo grupo. No início éramos apenas seis, mas chamávamo-nos de Comité Consultivo de Segurança e Estabilidade. Em 2002, foi efetivamente formalizado. A diretoria da ICANN se reuniu e disse: achamos que é importante ter um grupo composto por especialistas que entendam os fundamentos de como a tecnologia DNS, como as operações do DNS entendem esses fundamentos, se reúnam e vamos dar-lhes uma visão clara foco. Então foi isso que levou ao início do SSAC. A própria ICANN tem uma missão, e essa missão diz que está aqui no mundo para garantir a operação estável e segura dos sistemas de identificadores exclusivos da Internet. Essa estabilidade e segurança é o que conduz à missão do próprio SSAC. Então, qual é o nosso papel? Analisamos assuntos, questões relacionadas à segurança e à integridade de todos os sistemas de nomenclatura e alocação de endereços da Internet, e compilamos um grupo de especialistas que entendem desse tipo de questões. Nós nos reunimos, trabalhamos juntos e depois damos conselhos. O conselho é nominalmente dirigido ao conselho, mas na verdade é dirigido ao conselho e à comunidade. Aqui está o que é realmente interessante sobre o que fazemos. Somos um comitê consultivo. Nós apenas fornecemos conselhos. Nosso conselho: a diretoria da ICANN deve ouvi-lo. Eles podem simplesmente ignorar isso. Eles podem jogá-lo fora se assim o desejarem. Não há estatuto nem requisitos para que a diretoria da ICANN aja de acordo com nossos conselhos. Este é um recurso realmente excelente porque, deixe-me dizer, o que significa é que nós, o SSAC, temos uma enorme responsabilidade de que, quando fornecemos aconselhamento, ele

seja respaldado por dados. É apoiado por coisas reais que observamos no mundo real. Não é só um monte de gente que quer se unir e dizer que o céu está caindo. Nossa credibilidade é baseada na modelagem baseada em dados, na análise baseada em dados ou em algumas análises baseadas na experiência que elaboramos. Isso significa que também não estamos limitando a ICANN e a diretoria a cada um de nossos conselhos e recomendações porque, em alguns casos, nossos conselhos podem ser muito fortes e podem não ser implementáveis dentro do sistema da ICANN. Noutros casos, o nosso conselho pode não ir suficientemente longe. Isso proporciona alguma margem de manobra, mas o mais importante para nós no SSAC é que, por sermos um comitê consultivo, sem o poder de forçar algo a acontecer dentro desta comunidade, isso eleva o padrão para fornecermos conselhos que sejam realmente decentes. implementável, que se baseia em dados e factos. Este slide contém muitas palavras, mas vou me concentrar em apenas algumas coisas. O que realmente fazemos? Nós nos envolvemos com a comunidade técnica, a comunidade técnica focada na infraestrutura DNS, focada nos requisitos de segurança. Mas quando digo comunidade técnica, também me refiro ao pessoal político. Também me refiro às pessoas que estão envolvidas com a lei. Por isso, nos envolvemos com um grupo de pessoas que têm grande interesse em DNS e segurança de DNS. Depois de interagirmos com eles, analisamos os riscos e as ameaças aos sistemas de nomenclatura e alocação de endereços da Internet. Formamos grupos dentro do SSAC e muitas vezes não temos todo o conhecimento necessário, então iremos e entraremos em contato e pediremos e convidaremos

especialistas para trabalharem conosco. Isso significa que as pessoas que estão no SSAC, que trabalham com o SSAC, muitas vezes estão lado a lado, tendo conversas profundas com pessoas que estão realmente construindo as tecnologias, os protocolos, os sistemas que fazem a Internet, o DNS como conhecemos hoje., correr. Feito isso, coordenamos com as diversas entidades técnicas e outras, e chegamos a conclusões sobre qualquer tema que estejamos analisando. Então deixe-me dar um exemplo. Recentemente, vimos o que acontece com os nomes de blockchain que estão no blockchain. O que acontece com outros tipos de nomes que estão evoluindo no ecossistema geral? Qual é o impacto que isso tem no DNS. E reunimos um grupo de pessoas que têm interesse e experiência. Passamos cerca de um ano trabalhando nisso e publicamos um relatório. Esse relatório é público e contém observações, recomendações, que está disponível para a comunidade consultar e também é direcionado ao conselho. Então essas são as coisas que fazemos regularmente. Isso é o que o SSAC faz, e se você observar quem é o SSAC, verá que na verdade faz parte da equipe de liderança do SSAC. Alguns de nós foram eleitos para fazer parte do SSAC como líderes. Eu sou a cadeira. Tara aqui à minha direita é a vice-presidente. Jim Galvin é nosso contato com a diretoria da ICANN, e Jeff Bedser e Barry Lieba também são dois estimados colegas que fazem parte da equipe de liderança. Mas a forma como olhamos para isso é o SSAC e o trabalho que fazemos não é possível ser feito sem as pessoas do outro lado da tela, a incrível equipe de suporte que temos. Então tem Steve, tem Danielle, Kathy e Moses, e entre todos nós, na parte inferior da tela, você vê o conjunto de habilidades e o conhecimento que

trazemos. Há outras cerca de 30 pessoas no SSAC que trazem outros tipos de habilidades, outros tipos de conhecimento e experiência. Resumidamente, não vou entrar em nenhum detalhe aqui. Esses slides serão disponibilizados para vocês, mas mostram a amplitude e a profundidade das questões que analisamos. Como você pode ver, a segurança do DNS é uma grande preocupação para nós. Fizemos muitas coisas sobre segurança de DNS, mas também escrevemos coisas sobre namespace global, domínios sem ponto, colisões de nomes, uso compartilhado de nomes de domínio, todos esses tipos de coisas. Acabamos de publicar uma reportagem sobre ter um nome que nunca deveria ser divulgado ao público, pois deveria ser utilizado para fins internos pelas redes. Então acabamos de publicar um relatório sobre isso. Temos nos concentrado em dados de registro, em nomes de domínio internacionalizados, em questões de aceitação universal, em variantes e em segurança de roteamento. Portanto, é uma ampla gama de interesses, mas se você observar, eles estão praticamente todos focados em nomes e números. Não comentamos se o spam é bom ou ruim. Não comentamos nas redes sociais, coisas que são itens de nível de aplicação. Nós nos concentramos basicamente em coisas que estão na camada DNS da Internet. Então esse é o SSAC. Para um certo tipo de geek, é muito divertido. E para muitas outras pessoas que recebem nossos conselhos, trabalhamos muito para torná-los digeríveis, acessíveis e explicáveis de uma forma que não seja depreciativa para as pessoas. Só porque você é um especialista não significa que precise mostrar sua experiência. Na verdade, a melhor maneira de ser um especialista é tornar esse conhecimento disponível e acessível ao maior

número de pessoas possível. Então esse é quem é o SSAC. Agora vou passar para a Tara falar, falei sobre o que é SSAC e o que fazemos. Tara está aqui para falar sobre quem é o SSAC.

TARA WHALEN: Olá. Como vice-presidente, também sou o presidente do comitê de membros, por isso estou muito feliz em falar com um grupo potencialmente de candidatos que poderão se tornar membros no futuro. Temos como um dos nossos objetivos diversificar a nossa adesão e estamos certamente a olhar para o futuro porque precisamos de sustentar a nossa adesão ao longo do tempo. É por isso que também fico feliz em conversar com pessoas que talvez estejam no início de seu relacionamento com a ICANN. Portanto, dependendo de onde sua jornada profissional chegou até agora, você já pode ter algum conhecimento a oferecer. Você pode estar em uma posição em um futuro próximo, ou talvez você esteja olhando um pouco mais adiante e pense que talvez o SSAC e o tipo de trabalho que eles fazem possam ser do seu interesse. Por isso, queremos nos conectar com você para garantir que essas oportunidades aconteçam. Então, hoje quero falar um pouco sobre nossos objetivos específicos de diversidade que estabelecemos e o tipo de habilidades e conhecimentos que procuramos, e também por que você pode estar interessado em ingressar e o que isso traz para você, e então de claro como você pode se conectar conosco e encontrar uma maneira de se juntar a nós.

SIRANUSH VARDANYAN: Tara, só para lembrar, com 10 minutos de antecedência, temos apenas 10 minutos.

TARA WHALEN: Claro, obrigada. Então aqui estão nossos objetivos de diversidade. Estamos realmente procurando perspectivas diversas e únicas. Como Ram salientou, temos uma grande variedade de tópicos que analisamos no âmbito da enorme missão de segurança e estabilidade. Temos desafios em toda a Internet global, mas lembre-se que estamos falando de global e que temos áreas de diversidade geográfica nas quais sentimos que somos fracos. Somos altamente tendenciosos em relação à América do Norte e à Europa, por isso gostaríamos realmente de estender nosso alcance a outras áreas do globo, África, América Latina e Ásia-Pacífico. Se tivermos aqui pessoas que talvez tenham formação acadêmica ou de investigação, podemos ter pessoas que são estudantes habituadas a fazer análise de dados, a fazer vários tipos de medição na Internet. Você tem conhecimento especializado que poderemos considerar muito útil para alguns de nossos trabalhos no SSAC. Também estamos analisando nosso equilíbrio de gênero, então ficarei muito feliz se pudermos ter mais mulheres para se juntarem a nós no SSAC também. Claro, estamos nos movendo para o futuro à medida que o tempo avança novamente. Gostamos de pessoas que possam estar em um estágio inicial de suas carreiras e que também estejam prontas e ansiosas para ingressar. Esta nuvem de palavras dá uma ideia da amplitude do que podemos procurar nos novos membros. Muitos, muitos tópicos aqui, tópicos muito técnicos retirados de algumas de nossas pesquisas de habilidades. Você pode ver que

obviamente existem aspectos de segurança e rede. Você pode ser alguém que trabalhou em uma área específica de networking, em uma forma específica de operações. Você pode ter experiência em aspectos de crimes cibernéticos de segurança ou gerenciamento de riscos. Muitos aspectos diferentes das questões de estabilidade da segurança são relevantes para nós e para o nosso trabalho. Você pode se ver em algumas dessas áreas de especialização. Dê uma olhada, especialmente nos documentos e no tipo de coisas que fazemos, e veja se há alguma maneira pela qual você acha que poderia contribuir. Novamente, por que você gostaria de se juntar a nós? Acho que Ram também discutiu algumas das partes divertidas e o que você pode querer fazer. Trabalhamos em questões de segurança muito cruciais. Se você gosta de se aprofundar e trabalhar em assuntos profundos e complexos, não falta esse tipo de trabalho no SSAC. Você poderá ampliar seu conhecimento para outras áreas relevantes da Internet em geral, como questões globais da Internet, questões de grande escala, trabalhando com vários especialistas em segurança nesses problemas. Você certamente achará isso bom para aprimorar sua carreira e aprofundar seus próprios conhecimentos. Há visibilidade para muitos formulários de segurança porque este trabalho tem um grande impacto globalmente falando. E, claro, a experiência é fornecida para melhorar a forma como os sistemas de Internet funcionam. E então você está aconselhando o conselho e a comunidade DNS em todo o mundo para tornar as coisas mais seguras e estáveis e ajudar a contribuir para a missão. Portanto, se esse é o tipo de coisa que você deseja fazer, recomendamos fortemente que você se inscreva para ser membro.

Temos materiais no site e um aplicativo on-line que disponibiliza todo esse material para você. Mas também salientarei que estamos tentando algo novo este ano e que temos um fórum aberto. Então temos uma sessão presencial que é na quinta-feira, Bloco 1. E é uma oportunidade para você interagir diretamente conosco, para nos dar um pouco mais de tempo para você ter uma conversa individual, para perguntar mais perguntas, para saber mais sobre as particularidades dos projetos em que estamos trabalhando e do trabalho que podemos estar planejando e apenas nos conhecer e descobrir como somos como um grupo de pessoas por perto porque nós saiba que isso também é importante. Portanto, encorajamos você a comparecer a essa sessão, mas também estamos disponíveis para você falar conosco a qualquer momento. Então, entre em contato porque adoraríamos entrar em contato com você. Obrigado.

SIRANUSH VARDANYAN: Obrigado. Fiquei emocionado com esta sessão e com a presença de vocês, ambos os grupos. Porque nós sempre, os bolsistas e a próxima geração temos muito interesse no aspecto da segurança e sempre gostamos de estar de portas fechadas. Mas agora estou feliz que suas portas estejam abertas para nós. Temos verdadeiros talentos aqui. E tenho certeza que depois de 15 anos de bolsa, finalmente temos um membro no SSAC, que vem do programa de bolsa, e estamos orgulhosos disso. Mas temos um enorme talento e capacidade neste grupo que tem interesse em vir e juntar-se. Então, obrigado pelas apresentações. E também gostaria de agradecer a Jeff por indicar o membro do comitê de seleção e mentor do programa de bolsas. Não sei

explicar o quão importante é ter a sua expertise na seleção e na mentoria. Eu encorajaria o SSAC a também seguir essas etapas. Prometi à próxima geração que faria a primeira pergunta e vocês poderiam fazer a última, mas gostaria de cumprir minha promessa. Então a pergunta vem de você. Vá em frente. Pegue o microfone.

RASHID HASSAN: Obrigado pela oportunidade. Meu nome é Rashid Hassan. Sou um colega NextGen. Minha pergunta é para o Sr. Jeff. Eu tenho duas perguntas. Portanto, a primeira pergunta é uma questão técnica. No sistema DNS, existe um registro chamado registro CNAME, e muitas empresas possuem registro CNAME, e apenas o mantêm para fins de manutenção de registros ou alguns outros serviços. Porém, após a conclusão do serviço, eles esquecem de deletar o recurso, mas o registro DNS está sempre lá. E por causa disso, existe aquele ataque chamado sequestro de CNAME ou sequestro de domínio. Então os hackers fazem isso e dizem que eu hackeei o Google. Você não hackeou o Google. Você acabou de usar o CNAME. Então, no nível político, há algo, como, você recomenda algo às empresas ou à ICANN que, se eu não estiver usando um CNAME, por quanto tempo devo mantê-lo, o que devo fazer com ele e com que rapidez Eu deveria destruí-lo? Porque é apenas uma coisa técnica. E a segunda coisa é que, se estou ansioso para ingressar no RSSAC, tenho certeza de que há muitos white papers, recursos e muitas coisas. Você tem alguma coisa em versão infográfica ou em um breve resumo, posso entender o trabalho com muita facilidade se passar por ele? Isso é. Obrigado.

JEFF OSBORN: Obrigado pela pergunta. Deixe-me responder primeiro à segunda. Se você literalmente apenas pesquisar no Google, junte-se ao RSSAC Caucus, eu literalmente acho que você acabará ali mesmo. Está no site da ICANN, o que é realmente um ótimo processo. Existe um formulário fácil de preencher. Descreve o que procuramos, qual é o trabalho. Como eu disse, é um bom processo em que, se você não tiver atualmente o nível de habilidades que consideramos importante para que você seja um membro trabalhador valioso, será oferecida a você a posição de assistir e estar na correspondência listar e escolher em algum momento se você sentir que já descobri isso o suficiente. Volte e pergunte. Mas, em vez de uma função de aprendizagem, os membros reais são um grupo que realiza um trabalho real. Realizamos coisas reais. E então observá-lo é interessante. Então, eu literalmente apenas, se você pesquisar no Google, você estará lá em um segundo. Eu tentei ter outro aqui está uma maneira fácil de encontrá-lo. Google funciona. Quanto tempo você permanece com o CNAME, isso está muito fora da alçada do que o sistema do servidor raiz faz. E eu diria que você poderia jogar um gato e encontrar um especialista melhor do que eu. Wes, por exemplo, aqui, ou Peter, você quer ir até um microfone e atender? Peter é membro da convenção política do RSSAC e também do SSAC, eu acho.

PETER THOMASSEN: Muito rápido. Estou em um dos membros mais jovens do SSAC. E então, em relação ao CNAME, quando você não o usa mais, ele ainda aponta para o alvo porque o CNAME é essencialmente um registro de alias.

Portanto, o problema só ocorre se, sem você perceber, o nome do host de destino mudar o controle e for controlado por outra pessoa. Geralmente isso não acontece em um ou dois dias, mas se você esquecer de verificar, um problema poderá surgir mais tarde. Portanto, a recomendação seria: não tenha coisas que você não precisa. Não tenha portas em sua casa que você não precisa. E apenas remova o alias quando não precisar mais dele. Mas não é assim, se você deixar para lá, imediatamente se tornará um problema. Só se torna um problema quando o alvo muda o controle.

SIRANUSH VARDANYAN: Muito obrigado. E a última pergunta será do seu Esaú, e vamos resumir.

ESAU TUPOU: Obrigado. Sou membro da ICANN e falo por minha própria conta. Então, pelo que entendi, a internet começou como um projeto de defesa. Posso estar errado, mas é como um projeto de defesa. E não foi considerado o conceito de segurança desde o projeto. Mas então foi feito para troca de informações e também para comunicação. Mas agora muda tudo, como o crime convencional. Agora temos o crime cibernético e todas as outras coisas. Então, minha pergunta é para o SSAC: você também trabalha com as outras partes para a regulamentação, bem como para os direitos humanos e outras para garantir que a segurança seja segura? Obrigado.

RAM MOHAN: Muito obrigado. Essa é uma ótima pergunta. Fazemos a ligação com os governos, com o pessoal do governo. Temos alguns de nossos membros realmente trabalham para entidades governamentais. Mas também trabalhamos diretamente dentro da ICANN. Trabalhamos diretamente com pessoas do Comitê Consultivo Governamental, por exemplo. E dentro do Comitê Consultivo Governamental, existe um subgrupo chamado Grupo de Trabalho de Segurança Pública. Isso geralmente envolve pessoas que não são apenas reguladores, mas às vezes também são policiais ou pessoas assim, que estão focadas em garantir que haja estabilidade, lei e ordem na Internet também. Portanto, nos envolvemos regularmente e fortemente com eles. Também temos muitos de nossos membros presentes. Existem, em todo o mundo, equipes de resposta a emergências de computadores, CERTs. E então temos membros que se envolvem com isso. Ou existe uma organização guarda-chuva chamada FIRST, e eles também trabalham com ela.

SIRANUSH VARDANYAN: Muito obrigado. E vamos dar uma salva de palmas aos nossos apresentadores. Muito obrigado por ter vindo. E este é o grande final do segundo dia na ICANN. Com isso, essa reunião está encerrada, nos vemos amanhã na cerimonia de abertura.