SAN JUAN – Encontro conjunto: Diretoria da ICANN e RSSAC
Quinta-feira, 15 de março de 2018 – 10h30 às 11h30 AST
ICANN61 | San Juan, Porto Rico

KAVEH RANJBAR: Vamos começar em dois minutos.

David, sente-se à mesa, por favor. Muito obrigado.

Certo. Vamos começar a reunião. Jonne, por favor, a mesa principal.

Então, vamos começar a reunião.

Alguém do RSSAC ou da Diretoria não está na mesa principal? Porque temos cadeiras. Quem não estiver, por favor, venha para a mesa principal.

Bom dia a todos.

Bem-vindos à sessão pública entre a Diretoria da ICANN e o RSSAC. Vou começar esta reunião com uma chamada rápida, depois vamos ver a programação.

Será que eu começo pelo George? George, por favor, apresente-se.

GEORGE SADOWSKY: George Sadowsky.

DAVID CONRAD: David Conrad, CTO da ICANN.

AVRI DORIA: Avri Doria, Diretoria da ICANN.

RYAN STEPHENSON: Ryan Stephenson, RSSAC, DOD.

JONNE SOININEN: O Jonne Soininen, contato da IETF com a Diretoria da ICANN.

LITO IBARRA: Lito Ibarra, Diretoria da ICANN.

KAVEH RANJBAR: Kaveh Ranjbar, contato do RSSAC com a Diretoria da ICANN.

BRAD VERD: Brad Verd, copresidente do RSSAC.

TRIPTI SINHA: Tripti Sinha, copresidente do RSSAC.

CHERINE CHALABY: Cherine Chalaby, Diretoria da ICANN.

CHRIS DISSPAIN: Chris Disspain, Diretoria da ICANN.

BECKY BURR: Becky Burr, Diretoria da ICANN.

RAM MOHAN: Ram Mohan, contato do SSAC com a Diretoria da ICANN.

JEFF OSBORN: Jeff Osborn, membro do RSSAC.

DANIEL MIGAULT: Daniel Migault, contato da IETF com o RSSAC.

GORAN MARBY: Goran Marby, organização da ICANN.

KAVEH RANJBAR: Muito obrigado.

RUSS MUNDY: E Russ Mundy, contato do SSAC com o RSSAC. Fiquei sem ar, desculpem.

KAVEH RANJBAR: Bem-vindo, Russ.

BRAD VERD: Muitos membros do RSSAC que não estão aqui pediram desculpas. Muitos deles já estão voando rumo a Londres para a IETF. Só queria comunicar as desculpas deles.

KAVEH RANJBAR: Obrigado, Brad.

Antes de começar e responder às perguntas, quero definir o tom desta reunião. É uma reunião informal da Diretoria com o RSSAC. Preferimos manter o tom informal e ter um diálogo entre os membros da Diretoria e os membros do RSSAC. Já temos algumas perguntas. Vamos respondê-las. Só quero destacar que essas perguntas serão a nossa estrutura. Mas queremos dialogar. As opiniões mencionadas aqui podem ser de membros individuais do RSSAC. Isso precisa ficar claro. E também da Diretoria. Elas não vão levar a nenhuma decisão. Como sempre, as decisões serão tomadas com base em recomendações formais feitas pelo RSSAC à Diretoria. Acho que

é uma ótima oportunidade de usar esta hora para esclarecer qualquer dúvida ou comentário dos membros da Diretoria.

Dito isso, podemos passar para o próximo slide.

Estas são as perguntas da Diretoria da ICANN para o RSSAC. Basicamente, são duas perguntas. Vamos começar pela primeira.

Quais são os principais objetivos do RSSAC em 2018? Vou deixar os presidentes responderem.

TRIPTI SINHA: Obrigado, Kaveh. Obrigado também pelas perguntas.

Temos três objetivos principais para 2018. Vou começar pelo primeiro.

Como alguns de vocês já sabem, estamos trabalhando há aproximadamente três anos em algumas recomendações importantes para a Diretoria em relação à próxima fase ou à evolução do sistema do servidor raiz. Ele está em uso há décadas. O modelo é mais ou menos estático e não evoluiu.

Então, passamos bastante tempo investigando melhor esse modelo e resolvendo algumas questões que estão pendentes há muitos anos, como as medidas de responsabilidade integradas ao sistema. Perante a quem somos responsáveis? Quem são as

partes interessadas? Como é o financiamento? Como ele é sustentado? Como ele continuará crescendo e se adaptará à Internet, que não para de crescer?

Estamos perto de terminar a recomendação. Quanto ao cronograma, temos uma versão preliminar. Pretendemos ter uma versão bem próxima à versão final em maio, no workshop do RSSAC.

Nossa ideia é apresentar essa versão à Diretoria no workshop de vocês e fazer a votação e a finalização em junho.

Então, atualmente, salvo algum problema ou atraso imprevisto, vamos apresentar a recomendação no ICANN 62. Então, esse é o nosso foco principal no momento.

O segundo foco que temos é que, como vocês sabem, passamos por uma análise há pouco tempo. Essa análise ainda está em andamento. Provavelmente, vai terminar em abril. Depois dessa análise, teremos recomendações. E vamos trabalhar nessas recomendações com os comitês relevantes.

Além disso, temos a comissão do RSSAC, com foco nos problemas técnicos, tão numerosos e variados. Temos uns três trabalhos em andamento nessa área.

Então, no momento, esses são os principais objetivos para o ano de 2018.

CHERINE CHALABY: Tenho uma pergunta.

TRIPTI SINHA: Claro.

CHERINE CHALABY: Desculpe, Tripti. Em relação ao tempo, a recomendação será apresentada no ICANN 62. Sim? Você disse que quer enviá-la à Diretoria antes disso?

TRIPTI SINHA: Sim. A ideia é apresentar a recomendação para vocês no encontro de Vancouver, se conseguirmos incluir isso na programação.

CHERINE CHALABY: Excelente. Vocês vão entrar na programação. Sim, isso é bom.

KAVEH RANJBAR: Já pedimos um horário.

CHERINE CHALABY: Com certeza. Eu lembro. Peço desculpas. Sobre a análise do SSAC, desculpe, RSSAC. Você tem algum comentário sobre a eficácia da análise até agora? O que vocês acharam?

TRIPTI SINHA: Para nós, foi uma análise organizacional. A ideia era analisar o RSSAC, o Comitê Consultivo, a dinâmica desse comitê e a finalidade contínua dele dentro do ecossistema da ICANN.

Achamos que esse objetivo não foi atendido. Não foi uma análise organizacional do RSSAC e houve uma... posso falar da confusão que existe atualmente na comunidade sobre o que é o RSSAC, a função dele, e os outros membros da comunidade que formam o RSSAC, que definem o RSSAC, que são os RSOs, os operadores do servidor raiz. Mas nós sentimos que não foi uma análise organizacional em si.

CHERINE CHALABY: Estou perguntando isso porque várias partes da comunidade e grupos constituintes estão comentando sobre a eficácia das análises. Parece que é um tema comum, por isso, primeiramente, precisamos ver o número de análises feitas em um determinado ano e tentar dividi-las, fazendo com que cada uma seja mais eficiente em vez de fazer muitas coisas em um

ano e compactar... então, por exemplo, para o ano que vem existem novas análises planejadas. Certo?

O RSSAC apoiaria, praticamente todo mundo está dizendo a mesma coisa, analisar tudo de forma completa, ou seja, temos voluntários para fazer tudo isso? Temos os recursos para fazer tudo isso em um ano? Vocês acham que é melhor dividir tudo em dois ou talvez três anos e fazer menos, porém melhor?

TRIPTI SINHA: Concordo completamente com você. Na verdade, gostaríamos de fazer comentários. Achamos que vocês precisam dar um passo atrás, analisar o processo como um todo. E também a eficácia das análises. Qual é o objetivo e qual é o resultado desejado? Acho que vocês precisam de mais orientações para a forma como essas análises são realizadas. Garantir que elas não fujam do escopo, definir o escopo de forma bem estrita. E o tom do relatório, os relatórios precisam ser instrutivos e ter valor construtivo.

CHERINE CHALABY: Certo. Então, Goran -- então, sobre as análises, o plano de vocês é enviar o documento de consulta depois de -- qual é o plano? Como pedir mais comentários?

GORAN MARBY: Obrigado, Cherine. Aqui é o Goran.

Temos que falar sobre duas coisas diferentes. Uma são as análises definidas pelo estatuto. A cadência delas.

Quando começar, quando terminar. Essa é uma discussão.

É sobre isso que pretendo enviar informações, com o apoio da comunidade. Porque se formos fazer alguma coisa, seria uma mudança no estatuto em si.

O outro assunto que vocês estão mencionando... acho que também é uma pergunta importante, que foi feita não só por vocês: qual é o objetivo da análise?

Qual é -- o que vocês estão querendo com elas? Qual é a eficácia?

Sei que na OEC, essas discussões também já começaram.

Não tenho um plano para essa parte ainda. E não deveríamos também, porque isso veio da OEC para a Diretoria. Será um diálogo com a comunidade. Já ouvi isso várias vezes esta semana. Porque gastamos muito... desculpem. Investimos muito dinheiro e tempo nas análises em si. Algumas delas estão sendo feitas de forma organizacional há muito tempo. Acho que o At-Large está fazendo isso há quatro anos. Também há outra discussão.

Nesse aspecto específico, Cherine, preciso formular isso e conversar com a OEC, ter um diálogo com a Diretoria. Bom, o presidente está aqui. Ele pode continuar. Obrigado.

KAVEH RANJBAR: Temos o Brad e depois o Khaled.

BRAD VERD: Só queria dizer que o RSSAC está preparando duas respostas. Uma para o examinador independente esperando... compartilhar nossos comentários sobre a avaliação de forma que as recomendações que ainda têm que sair sejam, como Tripti disse, instrutivas e construtivas. Também temos o segundo feedback, estamos preparando nossa opinião sobre o processo todo para compartilhar com a OEC.

KAVEH RANJBAR: Khaled, por favor.

KHALED KOUBAA: Obrigado. Só quero compartilhar com você que a OEC teve uma discussão informal hoje de manhã, às 7h30. Todos os membros estão aqui também. Sabemos que os comentários da comunidade em relação às análises estão aumentando. Também sabemos da insatisfação de muitos grupos

constituintes sobre as análises, o processo delas, a forma como elas são realizadas. Com certeza, teremos diferentes ações. Como Goran disse, teremos ações em curto, médio e longo prazo.

A OEC também não poderá ter discussões agora, pois precisamos terminar esta reunião, digerir todos os comentários e feedbacks que estamos recebendo da comunidade e, depois, deixar a organização da ICANN trabalhar na estruturação de todos esses feedbacks em uma decisão bem embasada e baseada em evidências, que permitirá que a OEC apresente as recomendações à Diretoria.

Seremos muito ativos nisso porque vimos a importância do problema e também como é importante para a comunidade lidar com as análises de uma forma melhor. Mais uma vez, em longo prazo, também precisamos fazer a pergunta: qual é o impacto? Qual é o impacto dessas análises sobre a nossa organização? Mas essa também é uma questão de longo prazo. Obrigado.

KAVEH RANJBAR: Muito obrigado, Khaled.

Mais alguma pergunta? Cherine, por favor.

CHERINE CHALABY: Não é sobre as análises. Se houver tempo, gostaria de falar sobre as recomendações sobre a evolução do sistema do serviço raiz.

KAVEH RANJBAR: Por favor.

CHERINE CHALABY: Agora?

KAVEH RANJBAR: Sim.

CHERINE CHALABY: Certo. Então, o problema que está na minha cabeça é sobre os custos.

Não sei se vocês podem nos dar orientações sobre os custos para implementar as recomendações de vocês ou se podemos trabalhar juntos nisso. Porque o que está acontecendo no momento, e vocês viram isso em praticamente todos os grupos de partes interessadas, por exemplo hoje de manhã quando nos reunimos com o SSAC,

é que eles dizem que o volume de trabalho para eles fazerem recomendações é muito grande. Existe um problema de custos. Existe um problema de recursos.

E nós, da Diretoria, estamos do outro lado. As recomendações feitas para nós têm custo de implementação.

Essa questão é crítica, então vocês poderiam nos indicar os custos? Ou precisamos trabalhar nisso juntos?

TRIPTI SINHA: Então, acho que existem duas questões relacionadas aos custos. Uma é o custo de desenvolver as recomendações, no nosso caso, do comitê consultivo. Preciso dizer que fiquei chocado com a quantidade de trabalho, tempo e compromisso nos últimos três anos.

Não há custos associados a esse volume de trabalho. Mas quando entregarmos as recomendações, se elas precisarem ser implementadas, haverá um custo de implementação. Só a implementação. E existe outro custo, que é o custo do modelo. Quando houver um modelo operacional implementado, para operar essa nova infraestrutura e serviço. É, esse é o novo... qualquer que seja o modelo do sistema do servidor raiz. Esse, é claro, será um custo alto para as partes interessadas e assim por

diante. Então, na verdade estamos falando de três custos diferentes.

Vamos incluir números na recomendação? Não nesta versão, essa não era a nossa intenção. No entanto... Achamos que esse trabalho funcionará desta forma: nós entregamos a recomendação, a Diretoria lê, depois faz perguntas e nos pede mais detalhes, digamos sobre as finanças. Mais detalhes, assim por diante, depois analisamos essas questões de forma mais profunda e, em algum momento, decide-se se é sim ou não. Como eu disse, haverá custos de implementação se a resposta for sim, e depois o custo do modelo em si.

BRAD VERD: Sim. Acho que o processo de feedback que Tripti descreveu é entre a Diretoria e a comunidade.

CHERINE CHALABY: Certo. Mais uma pergunta sobre isso porque é importante. Isso afeta os sistemas de servidor raiz e, por padrão, os operadores do servidor raiz. A recomendação será consensual, com o consenso de todos os operadores de servidores raiz ou apenas uma recomendação do RSSAC sem o consenso total e a concordância dos operadores?

TRIPTI SINHA: Não, com certeza haverá consenso do RSSAC, e fomos muito explícitos dizendo que isso depende de cada RSO contido no RSSAC, que deve levar essas informações às empresas controladoras de forma que, antes que isso seja aprovado, elas saibam que os RSOs estão aprovando isso e apoiam esse modelo. Então, sim, com certeza haverá consenso.

Quando a recomendação for implementada, achamos que esse problema será muito maior que o RSSAC e o processo será orientado pela comunidade. Porque existem muitas partes individuais deste modelo que estão fora das nossas habilidades.

KAVEH RANJBAR: Muito obrigado, Tripti. Certo. Algum outro comentário ou pergunta da Diretoria ou do RSSAC sobre isso? Certo. Nada. Então, só queria dizer que, depois da chamada, chegaram Maarten, Lousewies, Lito, Ron, Sarah, Matthew e Khaled da Diretoria da ICANN. E Leon. Ah, sim. Desculpe.

Bom, passando para a segunda pergunta, bom, mais uma vez, a Diretoria pergunta ao RSSAC quais são os objetivos em longo prazo mais relevantes do RSSAC. Para dar mais contexto, basicamente é porque a Diretoria está trabalhando no plano estratégico para os próximos cinco anos, e o principal motivo para essa pergunta é receber comentários do RSSAC e dos nossos grupos constituintes, basicamente como contribuição

para o plano estratégico. Então, na verdade, essa é uma pergunta muito importante. Sei que isso também vai continuar no Panamá, mas por enquanto, queremos saber se o RSSAC tem comentários. Brad, Tripti.

BRAD VERD: Bom, acho que já falamos sobre isso. Acho que nossos objetivos mais relevantes em longo prazo seriam a implementação das recomendações que forneceremos no ICANN 62. Obviamente, teremos, vocês sabem... esperamos uma troca de ideias entre a Diretoria e, depois, um esforço muito maior com a comunidade. Esse é o início da conversa.

KAVEH RANJBAR: Muito obrigado. Como isso estava na apresentação inicial de Cherine, acho que também já ficou registrado como uma das próximas prioridades da Diretoria, certo, Cherine? Certo. Podemos passar para o próximo slide? Próximo slide. Sim.

Então, essas são as perguntas do RSSAC para a Diretoria. Vou começar pela primeira, que são as preocupações da Diretoria com o serviço da raiz ou, se há alguma pressão observada pela Diretoria, observada pelo RSSAC em relação aos servidores raiz. Ram.

RAM MOHAN: Obrigado. Ram Mohan. A preocupação mais significativa da Diretoria em relação ao sistema de servidor raiz é a ameaça de ataques de DDoS que podem sobrecarregar o sistema todo. A ameaça não é específica para o sistema de servidor raiz, é claro. Todos os serviços da Internet estão em risco. A Diretoria está conversando sobre as opções da organização da ICANN para ajudar a combater essa ameaça. Infelizmente, há poucas medidas que a organização da ICANN pode tomar com efeito imediato e direto sobre a ameaça.

A mitigação em prazo mais curto parece ser aumentar a capacidade do servidor raiz, mas isso tem um custo e certamente também tem um limite de tempo. Os operadores raiz têm a intenção de aumentar a capacidade e têm os recursos, o dinheiro, a equipe, etc. para fazer isso? Essas são algumas das perguntas que a Diretoria discutiu internamente. A Diretoria também está interessada em melhorar a responsabilidade geral dos operadores raiz.

Em relação à pressão que a Diretoria percebe sobre o sistema de servidor raiz, a Diretoria vê demandas não técnicas por mais operadores da raiz. A Diretoria sabe da necessidade de que a organização da ICANN tome todas as medidas razoáveis para reduzir as ameaças de DDoS. Por último, a Diretoria sabe do desejo da comunidade de aumentar a responsabilidade dos operadores da raiz. Essa foi a principal discussão da Diretoria.

KAVEH RANJBAR: Muito obrigado. Então, para dar um pouco de contexto para vocês, também, na nossa situação pública com a OCTO, eles nos apresentaram as propostas deles de mitigações da organização da ICANN ou possíveis soluções para mitigar alguns desses problemas, e eles também estavam conversando sobre as próximas etapas sobre em relação à ameaça.... essa proposta da OCTO foi enviada formalmente à comunidade técnica da Diretoria. No próximo encontro da comunidade técnica da Diretoria, que eu acho que será na semana que vem, sobre ameaças por e-mail, vamos conversar sobre como avançar. Acho que entrar em contato com o RSSAC e o SSAC é uma parte desse processo. Então essa ameaça vai continuar.

Enquanto isso, acho que o RSSAC já demonstrou interesse nisso e já houve algumas conversas e opiniões, alguns manifestando apoio, outros preocupações. Então, vou pedir para o Brad começar.

BRAD VERD: Sim, vou responder a várias perguntas e vou deixar o DDoS por último porque provavelmente será o diálogo mais intenso. Em relação à responsabilidade da Diretoria... à questão da responsabilidade da Diretoria e da comunidade, acredito que, como dissemos, estamos trabalhando nisso e consideramos que

esse tema será abordado nas próximas recomendações para a Diretoria. Detesto pedir para vocês esperarem, mas dedicamos um tempo considerável a isso. A ideia era analisar todos os pontos fracos e desafios que pudéssemos prever para garantir que o modelo resolveria todos eles. Isso é o que está levando mais tempo.

Em relação à demanda não técnica, acho que esse tema não será abordado especificamente no trabalho de evolução, mas vou dar as ferramentas para que a Diretoria faça a implementação necessária para tentar resolver isso. Esse é um desafio político, e nós somos um grupo técnico para... vocês sabem, fazer recomendações à Diretoria. É um tema que não está bem definido.

A capacidade... Desculpem, a capacidade para os servidores raiz, acho que... posso sinalizar o crescimento da plataforma atual que atende à raiz. Não faz muito tempo, acho que um ano, talvez um pouco mais, que estávamos sentados aqui falando de 600 instâncias no mundo todo. Agora, são mais de 950 instâncias no mundo todo. Então, o crescimento continua. Como vocês disseram, essa é uma das primeiras linhas de defesa para o risco de DDoS. Então, o que a OCTO preparou sobre o servidor de raiz "L" e compartilhou com a Diretoria e o RSSAC reflete exatamente o que está sendo feito pelos operadores de servidores raiz hoje em dia. Então, tudo o que

vocês veem lá especificamente sobre o L poderia ser aplicado a qualquer letra hoje em dia. É tudo o que é feito pelos operadores.

Em relação ao DDoS, acho, mais uma vez, que as ameaças sempre existiram. Essa não é uma ameaça nova para o sistema de servidor raiz. É uma ameaça existente, que é uma preocupação do RSSAC. É uma preocupação dos operadores de servidores raiz. Como vocês podem deduzir pela expansão e o dinheiro investido por todos os operadores para essa expansão da plataforma. Como vocês disseram, essa ameaça não é específica. Todos os usuários da Internet estão em risco. Em nossa discussão com a OCTO no início da semana, foi interessante porque percebemos que a raiz está correndo risco, como qualquer outra plataforma. Provavelmente há alguns TLDs que correm os mesmos riscos e poderiam ter maior impacto em menos tempo. Houve muitas discussões sobre isso, então deveríamos analisar esse assunto.

Com isso, acho que já abordei todos os pontos. Se eu tiver esquecido de alguma coisa, me avisem e vou tentar voltar ao tema, ou outra pessoa pode fazer isso.

KHALED KOUBAA: Obrigado, Brad. Cherine?

CHERINE CHALABY: Então, a pergunta que fizemos aqui dá origem a outra: por que agora? Vou explicar um pouquinho. Posso pedir a ajuda de vocês na resposta. Nossa missão sempre foi proteger e garantir a operação estável e segura do sistema de identificadores da Internet. O serviço de servidor raiz é muito estável desde a criação da ICANN, não é? E funciona. Acho que devemos ao RSSAC explicar por que de repente estamos mencionando esse problema, certo? Ou seja, ele sempre foi estável. É verdade que as nossas missões dizem que precisamos garantir isso. Não temos autoridade direta sobre os operadores de servidores raiz ou qualquer tipo de autoridade para fazer outra coisa. Então por que essa questão é importante agora? Ram, é bom você explicar as mudanças nas tecnologias que fazem com que essa questão seja pertinente agora e não antes.

RAM MOHAN: Obrigado, Cherine. Com a discussão na Diretoria, entendemos que a ameaça do DDoS em si não é nova. No entanto, o que chamou a atenção da Diretoria em relação a isso foi o fato de que agora temos ataques em escalas de terabytes, o índice de crescimento que parece estar superando o índice de crescimento de qualquer aumento de capacidade realizado.

Mais uma vez, reconhecemos que isso não acontece apenas no sistema raiz. No sistema do servidor raiz em si.

O segundo comentário que queria fazer é sobre a preocupação com a proliferação de dispositivos constantemente conectados à Internet que já vêm com vulnerabilidades e podem ser encurralados em botnets e outras ameaças de forma muito mais fácil que antes. Além disso, existem sistemas de código aberto que permitem que dispositivos desse tipo sejam encadeados em uma rede enorme de dispositivos de ataque, que poderiam chegar a sobrecarregar o sistema todo. Então, o desconhecido não é o DDoS em si. É o índice de aumento de ataques, que parece estar muito à frente dos métodos convencionais de resposta, que normalmente são o aumento da capacidade e a adição de mais largura de banda e mais hardware para responder.

KAVEH RANJBAR: Então, vou começar a conversa. Estou vendo representantes de seis operadores de servidores raiz aqui, das 12 organizações. Posso fazer uma pergunta direcionada a todos nós, operadores da raiz?

Algum de nós perde o sono com essas ameaças? Porque eu acho que, tecnicamente, todos entendemos a magnitude e a capacidade dessas ameaças ao sistema de servidor raiz. Mas

algum de nós perde o sono com isso? Sentimos que o céu está desabando, então... por favor.

JEFF OSBORN: Jeff Osborn da ISC. Somos os operadores do servidor de raiz F. Um dos pontos fortes da operação do servidor raiz é a diversidade de métodos. Então, todos nós somos organizações diferentes que fazem as coisas de forma diferente. Acho que a combinação deles tem uma grande força.

O ISC é uma das bases da Internet. Ele existe há muito tempo. Meus funcionários estão conosco há mais de uma década. Entre os quatro, são como centenas de anos de experiência na Internet. É uma organização enraizada.

Há um ano e meio, literalmente adicionamos uma grande magnitude de capacidade de largura de banda, primeiro fazendo o upgrade de todo o hardware existente em uso, depois, fazendo uma parceria com o CloudFlare, que é um provedor de grandes volumes de largura de banda praticamente no mundo todo. Estive em Katmandu há duas semanas, quando levantamos a instância do servidor de raiz “F” lá.

Os volumes de dados que tememos agora literalmente não são nada para os caras da CloudFly. Então, passamos de trabalhar sozinhos em um lugar onde um ataque de muitos gigas era algo

notável e causava preocupação a um lugar em que isso é apenas mais um item no registro. Não é um problema.

No relatório da OCTO, vi que parece que a ICANN, como operadora do sistema raiz, não está optando por seguir esse caminho. Isso é ótimo. Acho que o fato de ter opiniões diferentes é excelente.

Quero lançar uma ideia meio louca que minha Diretoria adora: conseguir dez mil pequenos dispositivos Anycast e espalhar pelo mundo para ter captações tão pequenas que uma tempestade de DDoS nunca teria chance de se formar, pois tudo seria absorvido por ânodos sacrificatórios, digamos, espalhados pelo mundo todo.

A força do DDoS é que muitas coisas se juntam para atacar um alvo. E a natureza do Anycast faz com que você seja absorvido pela instância local em vez disso.

Então, não é que não pensamos no assunto. É que não perdemos o sono com isso. Acho que estamos indo em uma direção interessante.

A última coisa que quero dizer é que se dissermos que estamos muito blindados contra ataques, nossos telefones vão começar a tocar e nossas pessoas de operações vão dizer que essa declaração provocou um ataque. Então, por definição,

precisamos ser humildes, e acho que vocês não vão gostar de receber essa mensagem.

KAVEH RANJBAR: Muito obrigado.

Temos Lyman, depois Ram e depois David.

LARS-JOHAN LIMAN: Lars Liman da Netnod. Também operamos uma das instâncias.

Quero agregar que também há outros mecanismos de defesa sendo implementados. Em relação a filtragem, relacionamentos entre os operadores de servidores raiz e os diferentes provedores de serviços de Internet que, involuntariamente são meios de ataque, no nosso caso, dos servidores raiz.

Existe uma rede inteira de pessoas e organizações com a boa intenção de manter as coisas funcionando. Esse é um recurso notável. Não estamos sozinhos nessa. Existe uma Internet inteira lá fora que quer nos ajudar.

Obrigado.

KAVEH RANJBAR: Muito obrigado.

Ram.

RAM MOHAN: Obrigado. Quero falar de algo que já foi dito, sabem... o relatório que a OCTO apresentou falava sobre a expansão da instância do servidor de raiz "L", dos L-clusters e L-singles, etc., que esse tipo de expansão poderia ser aplicado a todas as outras letras.

Dentro da Diretoria, não está claro que existe o mesmo tipo de investimento ou o mesmo foco no planejamento de capacidade. O que não significa que isso não aconteça. É que não há divulgação.

A outra preocupação é que podemos passar de ataques na escala de 1,7 terabits por segundo para ataques em escala de 5, 7, 10 terabits.

A preocupação é: O planejamento é adequado? O gerenciamento de riscos é adequado? Que tipos de mecanismos de mitigação existem para os encarregados de operar o sistema de servidor raiz?

Acho que esse nível de diálogo e esse tipo de educação da Diretoria seria extremamente útil para reduzir algumas das preocupações que existem.

Outra coisa que poderia ser útil e ajudar em relação à questão de responsabilidade seria um relatório geral sobre os

investimentos ou as expansões de capacidade, etc. Talvez em algum metanível uniforme, que possa ser disponibilizado para a comunidade, porque a Diretoria não é a única que recebe essas notícias. Os membros da comunidade também. Obrigado.

KAVEH RANJBAR: David, o comentário é em relação a este tema? Alguém quer responder diretamente? Sim, se a resposta for para esse tema, por favor.

BRAD VERD: Algumas ideias. Primeiro, só quero dizer que esses questionamentos são bastante operacionais, que é uma linha de questionamento razoável, mas quero dizer que essa é uma linha de questionamento operacional, e o RSSAC não é necessariamente responsável pelo RSSAC. Também foi dito que não existe responsabilidade operacional fora do L.

Não quero perder de vista o fato de que estamos fazendo um trabalho de evolução. Nosso objetivo é abordar a governança organizacional e a responsabilidade operacional nesse modelo. Sei que isso é para o futuro e que o existe um risco imediato que está provocando essas perguntas operacionais. Entendemos que existe uma necessidade imediata e que temos uma resposta futura, se é que isso faz sentido. Não quero perder isso de vista.

Falando verdadeiramente como operador da raiz, não como pessoa do RSSAC, não sei o que acho... Com certeza, não sei o que a minha organização acharia de um metarrelatório mostrando capacidade e investimentos porque isso não seria bom, pois no caso da infraestrutura é essencial não dar informações para os vilões. Isso é algo que deve ser levado em conta nessa discussão.

Sabem, não quero publicar exatamente qual é a minha capacidade. Várias coisas não deveriam ser publicadas. Isso deve ser levado em conta em nível operacional, não em nível de políticas, esse é um risco que precisa ser levado em conta pela Diretoria, pela comunidade, pelas pessoas que perguntam sobre os avanços que estamos fazendo.

RAM MOHAN: Rapidamente, Kaveh.

Brad, a Diretoria está totalmente de acordo com essa perspectiva. Todos sabem que a ideia não é oferecer informações para que os vilões saibam o que fazer e como atacar.

Parte do questionamento ou parte do trabalho que precisamos fazer juntos, que me lembro bem de uma das discussões em um dos workshops da Diretoria é a seguinte questão: Por exemplo,

caso haja um ataque significativo e uma parte da raiz caia, quem será responsabilizado diante de algum comitê? E que perguntas serão feitas? A pergunta que será feita é: Vocês sabiam que poderia haver uma ameaça? Vocês sabiam que havia uma ameaça significativa que poderia derrubar o que é visto como o centro da Internet? O que vocês fizeram em relação a isso?

Acho que parte do que estamos tentando fazer é colaborar e trabalhar para chegar a respostas reais para essas perguntas, tendo em mente que, do lado operacional, não queremos expor as coisas que vocês estão fazendo. É um trabalho importante. É um trabalho bom. Não queremos expor tudo isso. Mas, ao mesmo tempo, a Diretoria gostaria de ter visibilidade e confiança de que esse trabalho está acontecendo, não só ouvir "confiem em nós, estamos trabalhando", certo?

Isso é o que está acontecendo. Desculpe ser tão direto. Mas essa é a natureza do que realmente está acontecendo das discussões da Diretoria.

KAVEH RANJBAR: Obrigado. Alguma resposta? Tripti, pode falar.

TRIPTI SINHA: Ram, tenho uma resposta em duas partes para a sua pergunta. Primeiro, entendemos completamente a posição da Diretoria,

de que vocês precisarão de argumentos. Respeitamos isso. Entendemos isso. As ameaças sempre existiram, sejam nucleares, militares ou cibernéticas. Estamos pensando nisso e continuamos melhorando nossas operações na medida do possível. Entendo que precisamos oferecer algum tipo de relatório agregado a vocês, dizendo o que os operadores de servidores raiz estão fazendo, de forma geral. Concordo totalmente com o Brad, que não queremos expor informações internas sobre o que estamos fazendo, mas com certeza podemos gerar algum tipo de relatório agregado para assegurar vocês, isso está na nossa pauta. Está na nossa pauta há décadas. Não apenas em relação aos sistemas de servidor raiz, mas sim em relação a qualquer tipo de ameaça.

Esse é o motivo pelo qual estamos trabalhando nessa recomendação, porque sabemos que precisamos de responsabilidade. Quem são as partes interessadas? Estamos morrendo. Estamos aqui desde o nascimento do sistema de servidor raiz. Algum dia, não estaremos mais aqui. Precisamos entregar tudo isso a alguém e criar esse novo modelo, por isso estamos fazendo isso. Mas, paralelamente, continuamos fortalecendo o serviço. Estamos fazendo isso de forma diferente. Somos 12 organizações diferentes. Existe uma diversidade enorme. Mas não sei se isso responde à sua pergunta.

KAVEH RANJBAR: Pedi a permissão do David para continuar com esse assunto antes de chegar ao comentário dele. Temos mais dez minutos para dedicar a esse assunto.

RAM MOHAN: Rapidamente. Acho que não podemos resolver essa questão aqui, mas isso é o começo de um diálogo muito bom. Vou falar por mim, não pela Diretoria.

Falando por mim, precisamos de um mecanismo para continuar esse diálogo de forma constante, não apenas nas sessões, mas entre as sessões, porque, como vocês disseram, sabemos que essas ameaças existem e que também existem outras, certo? Acho que precisamos de algum mecanismo que fosse um círculo contínuo, não temos isso ainda.

Eu estou muito disposto a encontrar uma forma de fazer isso, pois a capacidade de poder sentar e dizer: “olha, não estamos preocupados só com a parte operacional, mas também com o fato de que, se algo realmente acontecer com as operações, o que vocês vão dizer é verossímil e comprovável por fatos? Sabem, isso só pode acontecer quando o diálogo é contínuo.

BRAD VERD: Só quero adicionar uma coisa, rapidamente. Seu comentário dizendo que agora é 1,7. Que mais tarde serão 5 e 6 terabits. Há uns cinco, seis anos, estávamos falando sobre como seria um ataque de um terabit e como nos planejamos para isso e tentamos lidar com isso.

Essa é a relação normal entre os heróis e vilões, certo? Eles dão um passo e nós respondemos. Os vetores de ataque estão sempre mudando. Não existe uma bala de prata que sirva para tudo. Estamos sempre adicionando ferramentas novas à caixa de ferramentas para lidar com os vilões.

KAVEH RANJBAR: Muito obrigado. Outros comentários ou perguntas sobre isso? Sim, por favor.

RAM MOHAN: Rapidamente, percebi que o Lito está aqui também. Lito e eu somos copresidentes do Comitê de Riscos da Diretoria.

O tema principal aqui é a abordagem ao gerenciamento de riscos, certo? O que importa não é saber quais são todas as soluções, mas sim entender que os riscos e os contra-ataques foram pensados e ter um certo grau de tranquilidade de que nossas respostas terão uma chance razoável de sucesso.

KAVEH RANJBAR: Certo. Se não houver outros comentários, David, pode falar.

DAVID CONRAD: Sim, só queria esclarecer uma coisa. A ideia do relatório que a OCTO forneceu à Diretoria e, subsequentemente, ao RSSAC era mostrar um conjunto de opções que a organização está considerando no contexto da operação do servidor de raiz "L" e também opções relacionadas à proteção do serviço de raiz. A ideia não era indicar que foi tomada uma decisão sobre abordagens específicas que devem ser aplicadas.

Demos algumas sugestões, com a opinião da OCTO sobre as abordagens racionais que deveriam ser aplicadas, mas algumas das opções propostas nesse documento implicariam gastos enormes de recursos.

Então, eu adoraria definir a que as verbas são dedicadas, mas essa não é a minha função.

KAVEH RANJBAR: Muito obrigado.

Podemos passar para o próximo assunto? Se houver comentários ou perguntas, tudo bem.

Então, a segunda pergunta do RSSAC para a Diretoria é basicamente sobre a perspectiva da Diretoria em relação ao plano proposto para a renovação da KSK. Bom, vou passar a palavra para o David responder a essa pergunta sobre a renovação da KSK.

David.

DAVID CONRAD: Então, a situação que estamos enfrentando agora é que temos dados que sugerem que quando implementemos a renovação da KSK, alguma porcentagem dos resolvedores ficarão mal configurados e falharão caso a validação das DNSSEC esteja ativada. Mas esses dados não são muito úteis porque o design original da renovação da KSK enfocava os usuários que seriam impactados, sugerindo que no máximo 0,5% dos usuários sofreriam um impacto negativo com a renovação da KSK. Se isso acontecesse, voltaríamos atrás.

Então, no momento, estamos tentando conseguir mais comentários públicos sobre um plano proposto para avançar com a renovação em 11 de outubro de 2018, independentemente dos dados que recebemos nos 8145 relatórios de resolvedores.

Acho que parte do problema é qual seria a opinião do RSSAC sobre esse plano proposto, e o que o RSSAC proporia para reduzir as preocupações e os riscos associados à renovação.

KAVEH RANJBAR: Então, repetindo o que também foi dito no encontro com a OCTO, quando o cronograma foi apresentado, em maio a ideia é... Há muitas chances de que em maio haja uma resolução da Diretoria pedindo que o RSSAC e o SSAC também façam recomendações, apenas porque é assim que funciona. Algumas etapas devem ser aprovadas para que a Diretoria possa apresentar essa resolução. Então, enquanto isso, nada impede que o RSSAC ou o SSAC comece a trabalhar na recomendação ou, se tiverem comentários ou opiniões sobre esse processo, que apresentem uma recomendação. Lembrem disso e, se necessário, programem trabalho.

Muito obrigado.

A última pergunta na verdade é sobre o cronograma. Bom, a pergunta foi feita e, enquanto isso, houve algumas recomendações que o Brad vai explicar.

BRAD VERD: Sim. Acho que essa pergunta foi superada pelos fatos. Essa pergunta era uma resposta à pergunta da GNSO, que buscava

respostas dos diferentes Comitês Consultivos sobre a adição de mais de 25 mil nomes ao espaço de nomes.

O RSSAC respondeu, o SSAC respondeu, e essa pergunta foi criada para a Diretoria muito antes dessas transações.

Então, há menos que haja algo para adicionar sob o ponto de vista da Diretoria, acho que essa pergunta foi superada pelos fatos.

KAVEH RANJBAR: Muito obrigado, Brad.

Outros comentários sobre esse assunto?

Certo. Caso contrário, há algum outro assunto que a Diretoria ou o RSSAC quer compartilhar ou discutir?

Ou, como ainda temos um pouco de tempo, alguém na sala, embora esse encontro esteja aberto para observadores. Mas se houver algum comentário real relacionado ao RSSAC ou à relação da Diretoria com o RSSAC, será um prazer acomodar isso.

Certo. Bom, não estou ouvindo nada, então vamos concluir esta sessão.

Muito obrigado por participar. Obrigado.

[FIM DA TRANSCRIÇÃO]