CLAUDIA RUIZ: Bom dia, boa tarde e boa noite para todos. Bem-vindos a esTa Chamada Mensal da LACRALO, 18 de abril de 2022 às 32h00 UTC.

No canal de espanhol estão Augusto Ho, Alfredo Lopez, Carlos Aguirre, Geraldo Martinez, Gilberto Lara, Hannah Frank, Harold Arcos, Laura Margolis, Rodrigo Saucedo, Sergio Salinas Porto e Virkson Acosta. Está Claire Craig no canal de inglês e Sindy Obed no canal de francês. Sylvia desculpa-se, Sylvia Herlein Leite e Dev Anand. E quanto ao pessoal estou eu, Silvia Vivanco... e eu, Claudia Ruiz. E os intérpretes são Marina e Paula no canal de espanhol, Esperanza e Bettina no canal de português e Jacques e Claire no canal de francês. Também está aqui, Alberto Soto, que acabou de entrar.

E antes de começarmos, por favor, peço que digam os seus nomes, quando forem falar. E então, muito obrigada. E passo então, a palavra ao Augusto Ho.

AUGUSTO HO: Boa tarde, boa noite. E gostaria de agradecer a todos aqueles, que se conectaram nesta Reunião Mensal de Abril com os melhores desejos para esta reunião de hoje. Então, bem-vindos e passo a palavra a Claire, para que inicie a leitura e possamos aprovar a agenda de hoje.

CLAIRE CRAIG: Obrigada. Bem-vindos a todos para a nossa Chamada Mensal da LACRALO. Hoje, na agenda, temos o prazer de ouvir Nicolás Antoniello, quem vai falar sobre como podemos fazer com que o DNS seja mais

resiliente e seguro. Esta é a primeira de duas partes dos webinars. Depois da primeira, teremos perguntas. Depois um relatório da Diretoria da ICANN pelo León Sánchez e um relatório dos representantes do ALAC com o Carlos Aguirre. E outro projeto interessante, que o Sergio Salinas vai apresentar. É sobre uma atualização sobre o avanço do Planejamento do LAC Digital. Projeto que vai começar em maio. Depois teremos uma atualização regional com relatório sobre as eleições de uma representante regional e sobre as eleições de 2022.

Gostaria também de saber se vocês gostariam de conversar sobre outros assuntos interesse? Muito bem. Eu não vejo nenhuma mão levantada, portanto considero a agenda aprovada nesta reunião. Muito bem, então vou passar a palavra a Augusto Ho. Obrigada.

AUGUSTO HO: Obrigado, Claire. Fala Augusto Ho para os registros. E como foi mencionado na agenda, temos uma participação muito interessante e também esperada de Nicolás Antoniello. Vão ser aproximadamente 45 minutos em que ele vai informar-nos sobre como podemos fazer para que o DNS seja mais resiliente e seguro. Então, Nicolás Antoniello, pode falar. Bem-vindo.

NICOLÁS ANTONIELLO: Muito obrigado, Augusto. Obrigado a todos pelo convite, para compartilhar este espaço com vocês e pela oportunidade, que me dão para conversar sobre estes assuntos.

Sou Nicolás Antoniello. Trabalho na ICANN, como Gerente Regional para a América Latina e Caribe de Relacionamento Técnico. E hoje, vamos conversar sobre o DNS em geral e as extensões ou os protocolos padronizados, que foram agregados ao protocolo básico do DNS, para dar mais segurança e resiliência no sistema global. E também agregar características de privacidade na hora de trocar informações, privacidade de dados e das consultas feitas pelos usuários.

Não sei se posso compartilhar a apresentação, Claudia? E passando aqui, desde aqui. Sim, agora é com a anfitriã.

DESCONHECIDO: Então, podem ver corretamente a apresentação?

NICOLÁS ANTONIELLO: Sim. Então, como fazemos com que o DNS seja mais resiliente e seguro? Se vocês quiserem fazer perguntas, não precisam esperar até o final da apresentação. As apresentações são mais interessantes, se o pessoal pergunta à medida que a apresentação é feita, também no chat. Eu não consigo ver o chat, mas se alguém perguntar alguma coisa no chat, peço que a Claudia ou outro leia a pergunta ou então, que a pessoa faça a pergunta no microfone. Tanto no meio da apresentação, quanto no final dela.

Esse parece um slide incompleto, mal feito, em branco. Eu queria representar aqui, o que acontece hoje na internet, quando queremos navegar até um site, antes de que o navegador possa descarregar dos diferentes lugares, todos os componentes do site, que estamos procurando. O que eu preciso saber é o endereço IP. E esses servidores

dos quais eu vou descarregar diferentes pedaços do site, vão iniciar a sua ação. E o servidor web não é único. É o principal, mas não é único. E os componentes dos sites web podem vir de diferentes servidores. E para um componente de autenticação para descarregar um texto, por exemplo. E o fato de visualizar um site significa que faremos diferentes consultas.

E quanto aos nomes de domínio, tendo o nome do domínio, que faz parte do URL e isso através de um endereço IP, descarregamos o site. E assim que começa a atividade do DNS.

E em nível de usuário, fazemos consultas. Uma consulta às cegas. O usuário não sabe o que está acontecendo. O terminal do usuário, como o celular, o computador envia ao servidor de nomes, o recursivo que vai fazer a busca do endereço IP correspondente ao nome, que é o **[inaudível – 00:09:41]** envia consulta ao DNS, ao servidor em questão. E vai acontecer uma série de mecanismos de buscas, o endereço IP. E depois o servidor DNS vai responder ao meu dispositivo com o endereço IP. Então, o navegador ou aplicativo poderá executar o restante das ações. Um site na internet, ele vai conseguir ser visualizado, exibido.

Isso é o que acontece, o usuário não consegue ver. Então, a priori, poderíamos dizer que o usuário também não está seguro e se esse endereço IP é o correto. E se houver algum ataque, por exemplo, que modificasse esse endereço IP, por exemplo. E que o meu cliente recebe, meu cliente vai ter acesso a esse site, pensando que é o original. Quando de fato, poderia ser um site falso, montado por um atacante, que conseguiu falsificar a resposta e enviar-me um endereço IP incorreto.

Em geral, nos sistemas aos quais estamos expostos ou que acostumamos utilizar na internet, temos serviços de e-mail, de calendário, de contatos que estão praticamente todos online. A agenda no meu celular não está no meu celular propriamente dito. Mas está online. Eu vou carregando contatos e isso fica em alguma nuvem online. E os meus dispositivos então, têm acesso a esses contatos.

Também temos serviços de bases de dados, dados de negócios, sobre as empresas em que trabalhamos, de clientes, dos funcionários das empresas, inventários. Também servidores e arquivos com informação financeira, documentos internos de organização da empresa com processos e procedimentos da organização, sistemas de controle e operação, como controle de equipamentos, como uma empresa de serviço, qualquer empresa de serviços. E não relacionada especificamente a internet. Mas pode ser de **[inaudível – 00:12:36]**. Isso requer sempre que haja sistemas de monitoramento. E que em algum ponto se interligam e tenham algum ponto de contato com a internet para poder fazer esse monitoramento remoto. Também mecanismos de segurança com senhas, controles de acesso, sistemas de registro de auditoria para administrar informações para auditoria de seguranças das empresas e muitos outros sistemas.

O bom senso também e ainda mais bom senso é muito importante. Eu vou falar sobre isso depois. E no Uruguai temos um ditado que diz “Às vezes, o bom senso é o menos comum dos sensos e devemos portanto, treiná-lo”. O bom senso, às vezes, não é tão óbvio assim para os outros e exige o treinamento para saber a que perigos, vou me enfrentar e como resolvê-los ou mitigá-los.

Todos esses elementos em geral e que estão online, começam antes de eu ter acesso. Começam com uma consulta ao DNS. Então, o sistema de nomes de domínio é um sistema distribuído. E quanto ao armazenamento da informação, que não está armazenada num único servidor do mundo, mas em vários. E a administração também não está concentrada. Há vários administradores. E uma administração distribuída e um protocolo projetado, para que isso funcione assim. Essas divisões administrativas do espaço em nomes de domínios são as zonas. Cada administrador de uma zona administra uma parte de todo o sistema global do DNS. Um administrador de qualquer zona pode delegar a administração de uma sub-árvore de sua zona, que tem uma estrutura de árvore invertida e a partir da raiz, temos os galhos. E num ponto das árvores, há folhas. Pode ser criada uma nova zona através da delegação de zonas.

E temos os servidores autoritativos e os recursivos. Não são resolvedores. Aqui deveria dizer, os servidores recursivos então. Servidores autoritativos são aqueles que armazenam a informação de cada zona, de cada domínio. E os resolvedores... servidores recursivos buscam informação no DNS em lugar ou representação do cliente ou dos dispositivos do cliente. Então não é o dispositivo, quem faz a busca, mas é quem entrega a consulta a pergunta. E o servidor recursivo faz a busca e quando tem a resposta, responde ao cliente final.

E por que estamos revisando tudo isso? Esse é um exemplo aqui, rápido, esse gráfico do sistema e um mecanismo – desculpem – de resolução do DNS aqui. Vamos pular rapidamente isso. Estamos revisando isso, porque depois, na apresentação, vamos começar a entrar em detalhe sobre todo esse mecanismo do DNS para ver as

ameaças mais comuns, onde elas agem e se existe algum mecanismo para solucionar as ameaças, evitá-las. Ou se não for possível evitá-las ou eliminá-las, talvez sim, possamos mitigá-las e talvez, haja algum mecanismo ou protocolo disponível para essa mitigação de ameaças.

Quando falamos em ameaças, nos referimos a esses três tipos mais frequentes de ameaças. Não são os únicos, mas sim, os mais frequentes. O *phishing* que é uma fraude, para a qual enviamos correios eletrônicos, que fazem de conta, que são empresas ou serviços renomados para induzir as pessoas a revelar ou informação pessoal. Enganam o usuário. Ele acha que está acessando um serviço conhecido, uma informação conhecida; quando de fato, o objetivo verdadeiro é induzi-lo a revelar informação pessoal, como senhas ou números de cartões de crédito, entre outros. Com a finalidade depois de utilizar essa informação do usuário, para depois inserir informações e extrair informações ou ter algum acesso não-autorizado a um sistema. Como ter acesso a uma conta de banco e então, fazer uma fraude.

O *malware* não visa o usuário, mas os dispositivos. É um software projetado especificamente, para interromper uma funcionalidade de um dispositivo ou danar o dispositivo, de forma provisória ou permanente ou não prejudicar ou danar, mas passando despercebido, obter acesso não-autorizado a um sistema informático para obter informação. Se eu quero extrair informação de um site e eu sou atacante, eu vou tentar passar despercebido. E isso é feito através desse *malware*, que vai me ajudar a ter acesso sem que os outros percebam. Ou domínios, que quando perceberem, já seja tarde demais. Os mais conhecidos são o *Ransonware*, *Keylogger, Rootkits*, os vírus etc.

E depois os *Botnets*, que é uma rede de computadores privados, infectado que eu, como atacante, monto. E é uma arma para fazer ataques a terceiros. E eu crio esse exército de dispositivos, inserindo software, em geral, *malware* nos dispositivos, sem que os usuários percebam. E quando decidir, no futuro, atacar como por exemplo, tipicamente é um ataque distribuído, eu envio uma ordem a todos esses dispositivos, que podem ser milhares, que estão comprometidos. Na internet, então envio uma ordem. Eu faço com que todos esses dispositivos façam algo simultaneamente contra uma terceira parte, como enviar dados sem importar o conteúdo dos dados, enviar todos esses dados a um terceiro. Milhares de dispositivos enviando dados a um terceiro. E esse terceiro vai ter saturação da banda. E esse serviço que ele dá, já não vai ser possível de concretizar. E há outros tipos de ataque mais elaborados, baseados neste tipo de *Botnet*.

Por que falamos de ameaça aos sistemas de nomes de domínio? Porque todos usamos esses sistemas de nomes de domínio. Então os objetivos dos atacantes é tornar vulnerável esse sistema ou outro. Então se eu interrompo os serviços de DNS, eu interrompo todas as transações. Porque já dissemos que tudo começa com o endereço de IP. Porque a gente nunca lembra dos números do endereço de IP. Então se eu fizer isso, então vou indispor as transações comerciais, todas as atividades da internet, pelo menos, na região onde esses serviços estão disponíveis, como governamentais e não-governamentais. Então interrupção pode ser mais ou menos problemática e pode até ser catastrófica. Como o caso dos sistemas de saúde, por exemplo, ou de energia, de água potável ou algum serviço de sustentação a vida. Então explorar o DNS pode enganar e fraudar os usuários.

Alguns vetores de ataque que são mais conhecidos são o registro de nomes de domínio de forma maliciosa. Aconteceu muito durante a pandemia. Então houve vários registros com informações contra a COVID e muita gente tinha acesso a essa informação. E também estava cedendo sem saber ou então, fazer o *download* de um arquivo, que era um *malware.* Então, ao mesmo tempo, eu estou acessando as informações e também recebendo um *malware*. O sequestro de serviços de registro ou resolução de nomes, alteração de dados do DNS. Então acessar os servidores autoritativos e mudar as informações, coleta de dados de sites comprometidos e para coletar dados de usuários e extração de dados é um pouco mais complicado. Eu não vou entrar em detalhes agora. Eu não vou falar de como são e como funcionam. Mas eles aproveitam que o DNS, que utilize um *Port* conhecido, como o 53 e utilize esse canal para extrair das organizações. Então, em geral, muitas organizações mantêm esse *Port* aberto, porque é o seu acesso ao DNS. Então muitos utilizam esse *Port* para extrair informações.

Então, esse slide apresenta uma visão geral de todo o ecossistema do DNS, os usuários, o estado que é o software, é o cliente de DNS do dispositivo que envia consulta ao revolvedor recursivo, que envia consulta aos autoritativos. E temos os registros e registradores de todo o sistema do DNS. Então aqui, em vermelho, mostra os pontos onde alguém possa atacar. São os pontos onde é possível haver ataques. Então, alguns mecanismos que foram adicionados ao DNS através de protocolos padronizados e eles funcionam em alguns desses pontos ou evitam ou mitigam os ataques.

A realidade, de fato, é uma corrida que nunca termina. Os atacantes sempre estão motivados a encontrar novas modalidades de ataque. Então as pessoas cometem erros. E quanto mais complicado o software é mais fácil. Então não há nenhum software, que não tenha nenhum erro. Então esses atacantes acabam corrigindo e é nesse intervalo, em que eles aproveitam. São esses, quem realiza ataques, que são muito criativos; então não é cavalo do comissário. Eles sempre estão adiante. O que nós precisamos fazer é a prevenção e fazer com que esses dispositivos funcionem. Então outra forma é mitigar também. Temos que aprender com isso e ver se algum mecanismo pode ser implementado, que evite isto. Então algum novo mecanismo de ataque sempre está esperando.

Há alguns mecanismos de resolução ou mitigação a serem considerados aplicados. O primeiro é manter múltiplos servidores autoritativos. O que quer dizer isso? Suponhamos que tenha autoridade para um determinado domínio. Por exemplo, NICOLAS.COM. Bom, na verdade, eu não tenho este domínio. Então, eu tenho o NICOLAS.COM, eu instalo um servidor DNS para o meu domínio. Eu tenho um arquivo de zona do NICOLAS.COM com subdomínios, LABORATORIOS.NICOLAS.COM, documentos etc., WWW.NICOLAS.COM para o meu site. Então, eu mantenho essa zona, que pode estar armazenada em um único servidor. Eu posso ter todas as informações num servidor autoritativo. Seria o mais simples. Mas em vez de ter todas as informações em um único servidor, ter vários servidores autoritativos idênticos. Todos terão as mesmas informações. Todos terão então, informações para o NICOLAS.COM.

Então, se há um servidor recursivo, que está tentando resolver a direção de IP de um dos meus domínios ou de alguns dos meus subdomínios, podem perguntar a qualquer uma dessas cópias, que eu mantenho do servidor autoritativo. Por quê? Porque todos têm as mesmas informações. Então, o que eu tenho aí, em vez de um único servidor, vários servidores com as mesmas informações. É o que se chama replicação de uma zona. E isso por sorte existe desde o início da padronização do DNS. É um mecanismo, que qualquer servidor, qualquer aplicativo funcione como servidor DNS, qualquer que um que utilize tal DNS e outros aplicativos para servidores autoritativos são implementados. E isto, esta replicação da zona está prevista e é relativamente fácil criar vários servidores e fazer com que todos os servidores tenham a mesma informação. Então, eu implemento as mudanças em um único servidor e todos os outros serão atualizados.

Segundo, esse servidor principal. Quais são as vantagens disso? Então, se houver um ataque a um servidor, se há uma falha ou um ataque num servidor, eu não fico sem serviço. Porque eu tenho outro servidor, que presta o mesmo serviço. Se eu tenho muitas consultas ou se alguém ataque o meu servidor e manda uma carga enorme de consultas, essa carga pode ser dividida entre meus vários servidores. Então, eu tenho maior capacidade de mitigar. Por exemplo, uma quantidade enorme de consultas. Então, isso faz com que esses servidores sejam mais resilientes.

Há uma técnica chamada NK, que também pode ser utilizada. E eu quero mencionar isso agora. Logo depois de manter vários servidores autoritativos. Mas depois disso, o mais comum é implementar essas duas formas, que eu vou mencionar. Então, ter vários servidores com as

mesmas informações, que servem a mesma zona. Então, quando se delega um domínio, o pai para criar a delegação filho, ele tem um registro que diz qual é o nome dos... o nome, desses servidores autoritativos, desse servidor principal. Então posso ter vários nomes de servidores. Então, quando um servidor recursivo busca a informação, então qual o servidor autoritativo para isso? Eu posso dar um único nome ou uma lista com N nomes, quantos eu queira. Então, o servidor recursivo vai tentar contatar um deles. Todos terão as mesmas informações, porque são cópias do domínio. Então, se ele não conseguir contatar com um, vai tentar o próximo. Então, tenho listas, tenho servidores múltiplos com IPs diferentes.

Por outro lado, a técnica do NK é definida como uma combinação de direcionamento IP e de roteamento. Então, quando chega o pacote, então ele encaixa, não precisa de nenhuma configuração especial de aplicativos, clientes. Eu preciso designar a mesma... o mesmo de endereço de IP a todos os dispositivos. Então, eu não tenho 2 servidores com 2 nomes diferentes. Então, eu tenho o mesmo endereço de IP.

Então, mas qual é que eu estou tendo acesso? Não importa, porque todos são cópias do mesmo. Eles mantêm a mesma informação. Então não importa a qual estou tendo acesso, porque todos são capazes de dar as mesmas informações.

Então, o que é um problema é se nós tivermos servidores diferentes, 2 servidores diferentes com o mesmo endereço de IP. Então, eu tenho servidores, todos com o mesmo endereço de IP. Esse servidor autoritativo e o roteamento vai decidir a qual servidor será enviado a consulta e ele vai responder. Então, são forma diferentes.

As vantagens do NK, ele dá redundância e resiliência a infraestrutura do DNS global, distribui a carga de consultas e respostas em vários servidores e reduz a latência. Porque eu posso localizar essas cópias, mais perto dos clientes. Então, eu posso ter esses servidores com o mesmo endereço de IP mais próximos do cliente. Então, a latência será menor. Porque a distância será menor e a resolução de nomes, portanto será mais rápida. E com isso, eu tenho maior solidez e ajudo a mitigar eventos, como ataques distribuídos e de negação de serviço, a estrutura do DNS. Essa técnica pode ser aplicada em servidores autoritativos e recursivos também. Eu posso usar o NK também para os recursivos. Eu não vou entrar em detalhes aqui, porque precisaria de uma outra palestra, maior conhecimento de roteamento etc.

Quanto ao que cada... servidores autoritativos, todos devem manter as mesmas informações. Então, isso já está previsto pelo DNS. Então, se pode ter cópias em um número indefinido de servidores. Então, cópias de servidores de DNS. Isso também dá resiliência aos nomes de domínio, não só... não a todos, mas a raiz de servidores. Vocês sabem que a raiz do DNS é onde começa toda a árvore do DNS. E a raiz do DNS, então simplificando muito. O dono da informação, o que administra a informação na raiz do DNS, a ICANN, a IANA, no escritório central da ICANN. Mas não é a ICANN, que presta serviço ao público. A ICANN administra e retém as informações e quem fornece essas informações são as organizações que mantêm servidores autoritativos na zona raiz.

Quantos? Duas organizações... 12, aqui temos 13 que estão listadas aqui. Temos a Verisign. Essas 12 organizações administram um servidor autoritativo para a zona-raiz. Isso quer dizer que são apenas 12 servidores autoritativos? Há milhares. Porque cada uma dessas

organizações utilizam a técnica do NK, que eu mencionei. Designam o mesmo IP a vários servidores. Então, tem várias cópias do seu servidor. O site **[inaudível – 00:39:58]**SERVICE.ORG que tem um mapa, que é atualizado de cópias de servidores-raiz em todo o mundo. Essa foto, eu fiz hoje. Então está bem atualizada. Então, segundo o site, hoje há 1.573 instâncias ou cópias de servidores autoritativos da zona-raiz. Algumas dessas são administradas por essas 12 entidades. Na nossa região aqui, temos 29 no norte e inclui o sul do Caribe, 29 cópias e 110 cópias na América Sul, mais para o sul, 266 que aparecem nos Estados Unidos, no norte do Caribe também. Então há centenas de cópias na América Latina e no Caribe. De quais servidores? De vários desses.

Então desta forma, para a raiz do DNS, onde sempre inicia a busca, eu tenho múltiplas cópias. Então, quando um resolvedor recursivo faz uma consulta, pode a ascender a qualquer uma dessas cópias e obter as informações. Então, ao termos cópias e estarmos próximos do cliente, se eu tenho menos latência, maior resiliência e mais capacidade de conter e mitigar os ataques. E no final das contas, melhor qualidade de serviço percebida pelos usuários. Então, há programas na ICANN e de outras organizações, que administram e mantêm os servidores da zona-raiz. Podem instalar uma cópia do servidor-raiz próxima dos usuários, no seu país, região etc. É uma forma de aumentar a resiliência e a segurança global do DNS.

Segurança. Vocês têm alguma pergunta? Estou indo muito rápido? O tempo está bom?

SILVIA VIVANCAO: Sim. Eu não vejo nenhuma pergunta, apenas um comentário, que eu posso passar depois e de forma privada para você ler.

NICOLÁS ANTONIELLO: Muito bem. Continuamos. O DNSSEC que é outra das características ou extensões de segurança do DNS, projetada para incrementar a segurança do DNS. Quando falamos em DNSSEC é segurança. E antes eu mostrei uma visão geral do sistema global do DNS. E aqui é onde o DNSSEC se encontra e onde age, que é entre servidores recursivo e o autoritativo. Então, esse é o cliente, envia a pergunta ao servidor recursivo, que busca a resposta entre vários autoritativos, começando pela raiz sempre. E quando já tem a resposta, a envia ao cliente. Este diálogo entre o recursivo e autoritativo pode ser assegurando, ativando o protocolo do DNSSEC.

Quem deve implementar o protocolo de DNSSEC? Quem são os participantes que fazem isso? Eles são aqueles que administram os servidores recursivos e os administradores dos servidores autoritativos. Não entra o cliente aqui.

O DNSSEC tem a ver com administradores de servidores recursivos e aos administradores de servidores autoritativos, então. Então o DNSSEC utiliza criptografia de chave pública e outro momento, vamos explicar isso. É um tipo de criptografia de mecanismos criptografar dados. E assinaturas digitais para oferecer autenticação de origem, que é por exemplo, quando eu faço uma consulta, sou recursivo e faço uma pergunta a um autoritativo e obtenho uma resposta do autoritativo, a autenticação de origem me permite ter certeza de que a resposta, que eu recebi pela internet, veio realmente do servidor que tem autoridade

para dar essa resposta. E não, de um site ou um servidor DNS ou um atacante ou de uma origem fraudulenta. E isso me certifica da origem.

E também o DNSSEC oferece integridade dos dados. Isso me assegura de que os dados, enquanto viajavam do servidor, do recursivo ao autoritativo, não sejam modificados. Não impede isso, mas só que quando os dados foram modificados e quando eu tiver o DNSSEC, eu posso realmente perceber se houve alteração ou não. Então, ter integridade, autenticação de origem e que é verificado, para que eu tenha a certeza de que essa informação é correta e não é falsa. E por exemplo, se estou acessando o meu banco; o DNS, o resolvedor me leva ao meu banco e eu não sei, nunca se estou entrando num site correto ou não. Não posso ver isso. Porque se houve alguma modificação no endereço IP, eu não tenho como perceber isso. O atacante faz um site idêntico ao original. E se eu acessar esse site falso, eu vou estar em problemas.

Quando o recursivo recebe resposta dos autoritativos e se a informação foi falsificada, o recursivo vai poder perceber isso e não vai dar o endereço IP ao cliente. O cliente vai receber uma mensagem de erro, não vai poder acessar. E o que vai acontecer é que o recursivo percebeu que houve manuseio de informações, com informações falsas e não vai dar acesso a você a esse problema. Para evitar, então esses tipos de ataques e também oferece proteção contra falsificação de dados do DNS e evita ataques de envenenamento do cache.

Não fornece confidencialidade. O que não faz o DNSSEC? Não fornece confidencialidade na troca de dados. Nem evita ataques de negação do serviço. Mas oferece proteção contra falsificação de dados, demonstrar

se os dados foram manuseados ou não. Não criptografa dados, nem oferece sigilo.

Quanto aos benefícios do DNSSEC, eles garantem a integridade e não-manuseio dos dados do DNS e oferece um mecanismo, eu não vou detalhá-lo aqui. Mas o DNSSEC também oferece um mecanismo para indicar ao cliente... Por exemplo, se eu faço uma consulta de um domínio, o site **[inaudível – 00:49:05]**. Como eu posso saber se essa resposta é certa ou não? Se o site existe ou não? O DNSSEC então, tem um mecanismo para que o servidor autoritativo desse domínio, que não existe, possa dizer ao recursivo que esse domínio não existe. E o cliente então, pode ter a certeza de que quando o servidor diz que não existe um site, isso é verdade. Isso me permite ter certeza de que um site não existe. Esses são os benefícios técnicos.

Quanto ao impacto nos diferentes membros do ecossistema, estão o usuário final. Isso agrega confiança para ele chegar ao site desejado ou correto, com o complemento HTTPS. E quanto ao registrante a mitigação de fraudes, mais proteção de marca. E também quanto ao registrador, vemos se cumpre com os padrões da indústria e satisfaz as demandas dos registrantes, para uma maior segurança. Isso para atrair e reter os registrantes focados na segurança e a reputação. Que é tudo aqui, para o DNS. E também os registros para cumprir com as melhores... eles cumprirem com as melhores práticas do setor e as demandas dos registradores, para dar uma maior segurança dos domínios.

SILVIA VIVANCO: Desculpe, Nicolás. Agora, já está acabando o tempo. Eu vou ler umas perguntas do Alejandro Pisanty para ir encerrando. Porque temos meia hora ainda para esta chamada. E temos outros assuntos para tratar.

NICOLÁS ANTONIELLO: Então, deixamos o restante para as próximas apresentações, que são outros mecanismos, que vamos ver na segunda parte.

SILVIA VIVANCO: Sim, claro. Vamos acompanhar a sua apresentação, que é muito interessante, com muito e bom conteúdo. Quanto as perguntas, a primeira é o DNSSEC tem ou tinha um efeito secundário não-desejado, que é facilitar a publicação de zonas inteiras. Como é que isso está sendo mitigado atualmente? Segundo. Qual é o tamanho daqui para frente, se podemos cobrir os custos para um administrador, para que ele possa implementar o DNSSEC. Quais são os custos e a complexidade?

NICOLÁS ANTONIELLO: Obrigado, Alejandro. Alejandro Pisanty, obrigado. Quanto a primeira pergunta sobre o efeito secundário não-desejável do DNSSEC, que facilitaria a publicação ou percorrer uma zona completa. Vamos ver se eu entendi bem a sua pergunta. É verdade que com esse mecanismo fornecido pelo DNSSEC incialmente e através do qual, eu posso ter certeza de que um site não existe, como eu comentei no exemplo anterior, ter certeza de aquilo que eu consultei não existe. Então, as primeiras implementações do protocolo que se chamava NSEC e este protocolo ou essa parte do protocolo lida com isso. E as primeiras

implementações permitiam que um atacante estivesse criando facilmente ou fazendo consultas facilmente e sistematicamente para percorrer uma zona e assim averiguar numa zona determinada, quais domínios existem e quais não. O mais é fácil é gerar palavras do dicionário, que façam sentido para os humanos de uma forma pseudoaleatória para ver se existem domínios associados a essas palavras. Pode perguntar por um domínio ou por outro e quando ele existir, vai ter uma resposta positiva. E quando não existir, vai ter uma resposta de que não existe. Então, eu faço toda uma cópia da zona, sem necessidade de ter acesso ao servidor para copiar tudo isso.

Também existe uma próxima versão desse NSEC, que é o 3, que modifica a maneira em que DNS responde, quando não há uma zona e reduz muito. Faz praticamente impossível fazer esse percurso, esse trajeto da zona, para obter informações. E também depende então, daquele que implementa DNSSEC também implemente o NSEC ou a terceira versão. Isso se aplica só para obter a informação de uma zona.

Os autoritativos por definição são zonas públicas. E às vezes, somos extremamente cuidadosos, especialmente os registradores são... os registros que administram os servidores autoritativos se cuidam muito de não revelar se os arquivos de zona. Mas os arquivos de zona são públicos por definição. Se não for assim, não cumpririam com os seus propósitos. Então, o fato de obter dados de toda uma zona, também não significa necessariamente, que esse seja um problema de segurança. Pode sim ser um problema, porque a pessoa está obtendo uma listagem de clientes. E isso claramente é um problema de segurança para um registro. Mas não é um problema de segurança a priori para o usuário, nem para o sistema de nomes de domínio. Mas é

uma preocupação válida dos registros e registradores. Mas sim ser um problema de segurança grande. De fato, arquivos de zonas que são públicos, como da zona-raiz, qualquer um pode descarregar a zona-raiz e outros arquivos de zonas que também são públicos.

Então, descendo na hierarquia, não necessariamente as zonas... todas as zonas... as zonas públicas representam problemas. E o NSEC3 ajuda a mitigar esse problema, fazendo com que seja tão difícil que... às vezes, não possa ser resolvido.

Quanto... qual seria o tamanho ideal, para que o administrador possa implementar o DNSSEC com custos e complexidade adequada? Se só implementar o recursivo não basta... se só implementar o recursivo não basta? Não, devemos implementar os 2. Implementar o DNSSEC em nível de recursivo, praticamente não tem sobrecarga técnica para os grupos de operações, que operam os recursivos. Hoje, por exemplo, se eu instalar um recursivo e qualquer software de recursivo entre os 3 mais conhecidos, eu sei que ele já automaticamente vem habilitado. Eu devo habilitar um comando para desativá-los. Essa já é uma complexidade que ele tem. Já vem com esse pacote. E eu preciso desativá-lo. Às vezes, aqueles que têm servidor... DNSSEC, talvez já tenham isso ativado automaticamente faz anos. Há coisas que no DNSSEC, a sobrecarga no servidor recursivo para implementar o DNSSEC se encontra frente a sobrecarga. E se não crescemos... nós devemos crescer com os clientes. E devemos monitorar sempre isso. Nenhum protocolo é implementado e deixado lá. E esquecer ele.

E quanto ao autoritativo, ele tem uma complexidade maior. Porque devemos manter as assinaturas; mecanismos de armazenamento

ativados, que podem ser mais complexos ou custosos, dependendo da criticidade que significa manter essa chave privada e secreta. A assinatura, às vezes, quando sou o administrador de um ccTLD, a cada dia pode ter centenas de novos domínios, que eu preciso assinar e habilitar. Então, preciso de um mecanismo online, automatizado para que quando um cliente novo cria um nome de domínio, uma assinatura seja gerada. Isso não é impossível, não é difícil. Existe muita ajuda para fazer isso. Há muita experiência de outros, que fazem isso faz anos. E também há muita oferta de treinamento acessível a todos.

E aproveitando a pergunta do Alejandro, na ICANN, convidamos qualquer operador para entrar em contato conosco e os acompanhamos ao longo de todo o processo em nível do autoritativo e do recursivo. Há operadores que querem fazer isso de forma privada. E não indicamos a eles o que devem fazer, mas sim vamos dar assessoria e vamos treiná-los e ajudá-los de uma forma mais ou menos eficiente.

E quanto aos autoritativos, sim. Há maiores custos, em geral de treinamento, custos operacionais e não, hardware. E quanto ao DNSSEC, ele deveria ser implementado por todos. É algo muito necessário, porque resolve um problema muito grande. E que se não for resolvido, o usuário não vai perceber.

SILVIA VIVANCO: Nicolás, peço desculpas. Excelente a sua apresentação. Eu vejo mãos levantadas. Mas precisamos avançar com a agenda. E nos comprometemos, para que em outra oportunidade, duas ou três oportunidades, possamos continuar com essa apresentação. E vamos continuar com a agenda. Sergio, Carlos, alguma pergunta sobre esta

apresentação? E se for assim, enviem a pergunta por escrito e nós as encaminharemos ao Nicolás.

NICOLÁS ANTONIELLO: Sim. Obrigado pelo convite. Eu respondo sempre as perguntas. E me comprometo a tomar nota delas e respondê-las na próxima. Obrigado pelo convite.

SILVIA VIVANCO: Obrigada de novo. Peço desculpas a aqueles que levantaram a mão. Mas vamos continuar com a agenda. Augusto Ho.

AUGUSTO HO: Obrigado, Silvia. Obrigado, Nicolás, pela participação. E já nos comprometemos para futuras apresentações. E temos agora, a participação de León Sánchez, quem vai apresentar um relatório da Diretoria da ICANN. León, pode falar.

LEÓN SÁNCHEZ: Obrigado, Augusto. Boa tarde, boa noite. Eu vejo que houve muita... houve muita atividade na Diretoria nos últimos meses. Tivemos a nossa Oficina da Diretoria antes da Reunião da ICANN. E tivemos diferentes interações com a comunidade durante a Reunião da ICANN. E iniciamos a oficina em 3 de março e revisamos algumas questões que tem a ver com análise de tendências, análise estratégica de tendências, que nos permite realmente medir como avança o sistema, como podem surgir questões que devem ser atendidas ou simplesmente observadas pela ICANN, como organização. E também determinar o grau de

participação, que a ICANN tem ou deve ter nesses diferentes cenários. Analisamos tendências, por exemplo, que podem parecer irrelevantes e até questões muito importantes, que podem significar um risco existencial para a organização. Como os sistemas alternativos de resolução de problemas com o DNS, que aparecem de partir de cadeias de blocos. Então analisamos se isso tem algum impacto sobre o DNS. E se é preciso continuar com essa conversa, interagir com aqueles que estão impulsionando esses tipos de sistemas alternativos, identificadores de sistemas de nomes ou redes da internet. Esse é mais um exemplo das diferentes tendências, que estamos analisando.

Também tivemos uma sessão, em que foram analisadas as tendências. E quanto as atividades entre os governos no ecossistema da ICANN, desde iniciativas que estão sendo apresentadas em diferentes países, principalmente na União Europeia e o impacto que isso poderia ter nas atividades da ICANN. E no segundo dia, tivemos também um exercício relacionado com o abuso do DNS. E conversamos também sobre as recomendações pendentes a respeito da revisão da segurança e estabilidade e resiliência. A segunda aqui é a revisão.

E também conversamos sobre a terceira edição de resiliência, segurança. Então na nossa reunião, nós definimos como seria essa revisão, para estarmos alinhados com as recomendações do ATRT3. Então a recomendação foi definir essa terceira revisão e aplicar as recomendações. E agora, no momento, isso está em pausa. E vai então, avançar na medida que avança a próxima versão do ATRT.

Tivemos uma sessão com o Göran Marby falando sobre o sistema de mitigação de ameaças ao DNS. E também foi apresentado um relatório

sobre abusos do DNS. E também continuamos com um segundo esforço de ver como priorizar as diferentes atividades, que estão na mesa da Diretoria e tentar alinhar isso com as prioridades da comunidade.

Bom, como... levando em conta as questões, que estão postas para a Diretoria, temos que priorizar em termos de recursos e relevância. Fizemos este exercício. E o que tentamos fazer é estabelecer as prioridades de forma unilateral. Mas o que nós fazemos como Diretoria, deva a participação da comunidade. Que a comunidade então, diga se está de acordo ou não com as prioridades e também em relação aos diferentes componentes da ICANN, como organização. Então, isso é mais uma questão para priorização.

E no último dia da oficina, vimos os resultados da Fase de Desenho Operacional para a próxima rodada. Então, conversamos sobre os resultados, vimos qual é a evolução disso para novas, próximas rodadas de novos gTLDs. Esta reunião já é ordinária. E foram aprovadas diferentes resoluções. Uma dessas decisões, eu já comentei. Então, o que foi uma terceira revisão. Também foi aprovada a Fase 2A do EPDP do Conselho da GNSO.

E também submetemos a consideração da Diretoria, a resolução de um caso de um processo de revisão independente, que envolve o gTLD .UL, porque houve uma controvérsia entre diferentes atores, que participaram do leilão, para adquirir esse novo gTLD. E o resultado desse confronto de interesses foi um processo litigioso. Não no sentido de levar isso a justiça ainda, mas de acordo com as nossas regras de tratamento das controvérsias, foi iniciado esse processo de revisão independente. Então, já foram feitas as recomendações e foram

submetidas a consideração da Diretoria. E foi resolvido que o Comitê de Mecanismos de Prestação de Contas deve revisar essa ou analisar essa resolução em detalhes e fazer diferentes recomendações a Diretoria. Então, isso ainda está em andamento. Será analisado. E obviamente, terei mais o que contar aqui.

E outra resolução que vocês já devem ter visto foi a constituição de um fundo de emergência para apoiar o acesso contínuo a internet, como resultado da crise, que está acontecendo na Ucrânia por causa do conflito na região. E foi decidido então, a conceder um milhão de dólares para trabalhar com agentes da região para manter o acesso contínuo a internet, nesta zona de conflito. E dentro da missão da ICANN, nós então, tentamos fazer com que em tudo haja grande transparência na gestão desses fundos.

E na semana que vem, teremos uma reunião em Los Angeles, pela primeira vez, em muito tempo, uma reunião presencial com líderes de diferentes organizações de apoio e comitês consultivos. E também uma reunião da própria Diretoria. Então, eu posso atualizá-los novamente, depois dessa oficina em Los Angeles e da reunião do Diretor e Vice-Diretor com as OAs e os CCs. Muito obrigado, Augusto. Eu não sei se há alguma pergunta ou comentário sobre o que eu falei.

AUGUSTO HO: Muito obrigado. Eu vou passar a palavra rapidamente ao Carlos Aguirre para o seu relato. Eu vou pedir que você seja breve, porque temos pouco tempo.

CARLOS AGUIRRE: Bem, muito obrigado, Augusto. Eu tinha levantado a mão para fazer uma pergunta ao León. Mas eu vou levar em conta, que temos pouco tempo. E eu vou fazer a pergunta em outra ocasião.

Bem, a ideia da minha intervenção nessa reunião é comentar o que fizemos no ALAC nos últimos tempos. Isso tem a ver com muitas coisas, que o León já mencionou. Essencialmente, isso é tratado dentro do Grupo de Políticas Consolidadas do ALAC, que se reúne todas as quartas-feiras. Então, eu pediria aos funcionários da ICANN, se poderiam postar aqui, o link para a reunião. Porque ela é aberta e todos podem participar, para que saibam o que está acontecendo. De qualquer forma, vou falar rapidamente, por causa do tempo.

Os temas desse Grupo de Políticas Consolidadas têm a ver com o uso indevido do DNS. Na última reunião, falamos sobre os registros maliciosos, blocos; o que aconteceram durante a pandemia e como mitigar esses ataques, essa forma de gerar situações complicadas pelos usuários. Estou falando fundamentalmente demais aqui.

Também tratamos do processo da revisão das políticas de transferência de domínio. E se colocou uma questão, que tem uma certa complexidade gerada pelo GDPR. Se falou também dos prazos dessas transferências, levando em conta frequentemente os interesses dos registros. E eu acho que nós, da nossa região, deveríamos aprofundar essa questão, para defender o interesse do usuário final da internet, o usuário individual.

E uma questão pessoal é que eu vejo que frequentemente, pessoas que são membros do ALAC, que por sua... o tempo... que estão há muito tempo neste grupo, são impactados por outros grupos, como GNSO e o

Grupo Comercial, o *Stakeholder* Comercial. Eu vejo muito interesse em custodiar os interesses financeiros dos registros e não, dos usuários finais. E eu acho que isso deve ser mais discutido nas nossas reuniões. E levantado nessas reuniões sobre o uso indevido da internet. Então, como facilitar as denúncias dos usuários, como fazer com que sejam mais simples ou gerar uma solução para o usuário, que teve os seus direitos violados.

Também falamos nos últimos tempos nesse Grupo de Políticas Consolidadas, o processo expedito de internacionalização de domínios e a aceitação universal, em quem estiver diferente um pouco de outros regiões, que solicitam caracteres diferentes, como Mianmar. E outro tema é o sistema de acesso padronizado, o SC SAC, que discutimos nesse grupo. E o que a há hoje, estamos discutindo e temos pouco tempo, por causa dos prazos, é a agenda da ICANN74, que já está aí.

O que nós vamos apresentar nessa nossa reunião, que também há outro problema que é uma reunião híbrida. Alguns vão participar da reunião presencial e outros vão participar de forma remota. Então, como fazer isso funcionar bem? Então, isso é um desafio. Isso é algo novo. Então, queremos saber como é que isso vai funcionar nas próximas reuniões da ICANN.

Outra questão e que será o primeiro da ICANN74, que a comunidade At-Large vai participar, que é no primeiro horário do primeiro dia. E que tem a ver com os interesses da GNSO, para falar dos procedimentos subsequentes. O interesse da GNSO é saber o que vai acontecer com a próxima rodada de gTLDs. Eu não sei se isso interessa aos usuários, mas

sim, para o Grupo Comercial. E é aí, que nós nos envolvemos. Porque nós, do Grupo de ALAC, temos que fazer recomendações.

Bom, isso é o que eu diria rapidamente, Augusto. Muito obrigado pelo tempo. E desculpem por ter sido tão breve.

AUGUSTO HO: Muito obrigado. Então, vamos pedir que Sergio Salinas nos fale do Planejamento do LAC Digital.

SERGIO SALINAS PORTO: Muito obrigado, Augusto. Boa noite a todos. Vou ser muito breve. E talvez, consigamos terminar a reunião no horário.

Temos a aceitação dos 3 temas. Na aceitação universal, queremos que haja 4 palestrantes. Teremos 3 já, que estão confirmados. Os outros 2 objetivos da internet, como serviço público essencial e a infraestrutura em zonas rurais já estão bem avançados. Eu acho que temos 24 atores de 12 países. E a nossa página já está quase pronta. E já temos currículos de painelistas da sociedade civil e do governo. Já estamos quase a ponto de ter um evento, que é no dia 17 de maio. Tem um nível comunicação bastante bom. Então, teremos maiores informações sobre isso vamos avançar.

Eu me comprometo, como eu disse na semana passada, de mandar um relato por escrito a toda a região. E aproveito para dizer ao meu amigo, Alejandro Pisanty, que amanhã, vou falar com o México. Era isso. Muito obrigado.

AUGUSTO HO: Obrigado, Sergio, por essa atualização e pelo o que está acontecendo. E desculpem. E vou solicitar a Claire, que nos fale sobre as eleições 2022. Pode falar.

CLAIRE CRAIG: Oi! As eleições 2022 têm 2 posições disponíveis para este ano. E temos isso aqui, na tela. Teremos a função no ALAC, representando a região D, que é a antiga Argentina, Brasil, Paraguai e Uruguai. E há uma função no NomCom, região A, que é América Central; o México, Belize, Costa Rica, El Salvador, Guatemala, Honduras, Nicarágua, México e Panamá.

Quanto a essas eleições, hoje, 18 de abril, hoje, vamos ter o anúncio das indicações. Entre 18 e 29 de abril, teremos o período de indicação. E são 10 dias uteis. E depois, teremos o prazo 6 de maio, para a aceitação das indicações. E 9 de maio a 12 maio são chamadas com os candidatos, se for desejado pelas RALOs **[inaudível – 01:28:12]**. E de 13 e 20 de maio, as eleições, que vão ser depois de 2 semanas, depois desse prazo.

E por último, na ICANN75 de 2022, os novos, eleitos, os membros do ALAC recentemente eleitos e líderes das RALOs assumirão as suas funções no final da Reunião da ICANN75, depois do encerramento da Reunião do *Board*, em 28 de setembro de 2022. Então, façam as suas indicações para a região D para o ALAC e a região A para a América Central, para o Comitê de Nomeação. Muito obrigada.

AUGUSTO HO: Muito obrigado, Claire, de novo. Está acabando o tempo. Vamos ter que encerrar a reunião de hoje. Ainda há alguns assuntos pendentes, mas vamos deixá-los para o próximo encontro.

Eu gostaria de lembrar, por favor, que respondam a enquete ao finalizar esta reunião. Mas temos ainda 2 minutos. A Vanda pode utilizá-los. Vanda, pode falar.

VANDA SCARTEZINI: Muito obrigada. Só queria informar que saiu tudo muito bem na reunião presencial em Washington. E de todo o Comitê do Nomeação, estivemos todos juntos. Éramos umas 14 pessoas. Resultados ótimos. Cada dia fazíamos testes às 7h00 da manhã, antes de entrar na sala de reuniões. Todos saímos de lá com boa saúde, sem nenhum problema. E a organização foi perfeita. Sempre, é claro, com as dificuldades correntes de transporte. Mas sem problemas, problemas graves. Então, também com o pessoal de Los Angeles. Tudo se saiu muito bem. Fomos realmente... trabalhamos de forma híbrida. E também com os 3 amigos, membros do NomCom, que não conseguiram o visto para poder chegar à reunião. E só puderam participar de forma remota. E foi muito, muito... tudo correu muito bem, bem organizado. Falamos tranquilamente. Também tiramos fotos com os membros. Então, o resultado foi excelente. Então, só queria mencionar que experiência-piloto foi bem-sucedida. Portanto, estamos mais tranquilos para a reunião em Haia. E é isso. Muito obrigada.

AUGUSTO HO: Obrigado, Vanda. E agora, vamos finalizar a reunião, Silvia.

SILVIA VIVANCO: Sim, eu peço a todos, que preencham, que respondam a enquete, que vai aparecer, assim que nós encerrarmos esta sessão de Zoom. Boa noite. Muito obrigada.

AUGUSTO HO: Obrigado.

SILVIA VIVANCO: Obrigada. Até mais.

[FIM DA TRANSCRIÇÃO]