[exibição de vídeo]

NARRAÇÃO: *Já imaginou se você não tivesse seu direito à liberdade de expressão respeitado? Se seus dados particulares fossem divulgados sem autorização? Ou se você tivesse a sua navegação filtrada por causa de interesses comerciais? A liberdade de expressão, a privacidade e a neutralidade da rede são fundamentais para a internet. E esses são apenas alguns dos dez princípios formulados pelo Comitê Gestor da Internet no Brasil. O CGI.br promove há mais de 20 anos a internet no país. Graças a ele, você tem constante inovação, segurança e diretrizes para o desenvolvimento da internet. Isso tudo é feito de forma colaborativa transparente e democrática.*

O comitê é formado por representantes de todos os setores da sociedade. Assim, as decisões são tomadas por meio do diálogo, com a participação de todos os membros, até que um consenso seja alcançado. Por esses e outros fatores, o modelo brasileiro de governança se tornou referência no mundo todo. CGI.br, por uma internet cada vez melhor no Brasil.

NARRAÇÃO: *Quando você registra um domínio .br, você está contribuindo para a melhoria da internet no Brasil. Pois cada domínio que usa o .br é registrado pelo NIC.br, o Núcleo de Informação e Coordenação do Ponto BR, que, além de registros de nomes de domínios, investe em análise e tratamento de incidentes de segurança, projetos de tecnologias de redes e operações, pesquisas que trazem indicadores sobre o uso das tecnologias da informação e comunicação, implementação de pontos de troca de tráfego local na internet, projetos que contribuem no desenvolvimento global da web e muito mais.*

Tudo isso porque o NIC.br é uma entidade civil de direito privado e sem fins lucrativos, que mantém uma estrutura de registro de domínio segura, estável e de confiança. E reverte parte do que você paga pelo seu domínio no desenvolvimento de infraestrutura, trazendo benefícios para todos que usam a internet no Brasil. Toda essa inovação, tecnologia de ponta, segurança e infraestrutura só é possível porque você tem um domínio .br. NIC.br, sempre em busca do melhor para a nossa internet.

SR. FREDERICO NEVES: Muito bom dia a todos. Sejam muito bem-vindos a 10ª Semana de Infraestrutura da Internet no Brasil, evento do NIC.br. Meu nome é Frederico Neves. Em nome do Comitê de programa do Grupo de Trabalho em Engenharia de Redes e do Grupo de Trabalho de Segurança, grupos do Comitê Gestor da Internet no Brasil, eu gostaria de dar as boas-vindas a todos para a 49ª Reunião do Grupo de Trabalho em Engenharia de Redes. E, para começar o dia

hoje, nós vamos ter a primeira atividade, que é a entrega do Prêmio Alberto Courrege Gomide 2020, na edição 2020, e, para apresentar o prêmio, eu gostaria de chamar Demi Getschko. Demi, por favor.

SR. DEMI GETSCHKO: Olá, bom dia a todos. É uma alegria estar aqui no 49º GTER, o próximo é o 50º, é importante a data, e esse Prêmio Alberto Courrege Gomide, essa é a segunda entrega dele... O Gomide, como todos conhecemos, era do time do GTER, era do time do pessoal da casa de máquinas, um caráter sensacional, uma pessoa absolutamente excelente, não é, e, além de tudo, um técnico absolutamente notável. E a gente resolveu, com o passamento dele, o falecimento dele, criar esse prêmio em homenagem, que é um prêmio que volta-se ao pessoal da área técnica, não é, o pessoal da casa de máquinas. Não é um prêmio envolvido com as pessoas que politicamente se movimentaram na área e tudo o mais, mas o pessoal que... É uma espécie de Prêmio Jon Postel, em que o pessoal reconhece alguém da comunidade deles como importante no desenvolvimento da Internet. Então, o primeiro foi entregue ao Vilson Sarto, e eu acho que esse prêmio é muito importante para consolidar o GTER e o GTS como uma comunidade, porque a comunidade elege, dentre os seus, alguém que é representativo, que participou de reuniões, que participou da criação disso, que participou de todos os movimentos importantes da área. Então, eu acho que o GTER e o GTS devem cuidar com carinho disso, não é? Esse ano, tivemos o Comitê de Programa elegendo o responsável, o receptor do prêmio, e vamos tentar expandir isso para ficar mais amplo ano que vem para quem quiser participar, e lembrando que será o 50º ano do GTER.

Então, para quebrar aí a surpresa, passo a palavra para o Danton, um dos antigos membros do GTER, que pode nos dizer um pouco mais sobre o que acontece esse ano. Danton.

SR. DANTON NUNES: Obrigado, Demi. Eu vou contar uma historinha. Nos idos de mil novecentos e bolinha, antes de a Internet se tornar tão ubíqua quanto água encanada, eu estava em um simpósio do SBRC, onde ela discorria sobre um experimento cujo propósito eu nem lembro mais, mas lembro que envolvia uma quantidade enorme de equipamentos. Na parte das questões, alguém da plateia pergunta: "Professora, por que a universidade não realiza esse experimento?". E ela responde gauchamente: "'Bá tchê'! Tu não sabe que universidade está mais pobre do que rato de igreja?". A partir desse momento, eu fiquei fã convicto desta que hoje recebe o prêmio Alberto Courrege Gomide, a Profa. Dra. Liane Margarida Rockenbach Tarouco.

[exibição de vídeo]

SRA. LIANE MARGARIDA ROCKENBACH TAROUCO: *O surgimento do CGI foi um movimento, digamos assim, organizado, o pessoal da área de Academia, alguns setores do governo, que*

percebiam um risco muito sério de que todo esse crescimento da rede Internet, que até então era acadêmico, mas que já começava comercial também, de ser abocanhado pelas administradoras de telecomunicações. Elas viam nesse segmento uma forte fonte de receita. E havia um movimento não tão sutil, não é, da Embratel, por exemplo, de entender que tudo isso estava dentro daquela lei de monopólio. Partes do governo perceberam isso e fizeram, então, esse esforço. Agora, só o governo, não é, encarar a Embratel, que, de certa maneira, era do governo, era uma coisa meio complicada, tá? Então, por isso envolver esse comitê multissetorial com outras vozes que davam respaldo, digamos assim, dizendo: "Não, é isso aí que o mercado precisa para o desenvolvimento do país".

SR. FREDERICO NEVES: E agora, com vocês, a Profa. Liane Tarouco.

SRA. LIANE MARGARIDA ROCKENBACH TAROUCO: Obrigada. Eu queria agradecer, estou muito tocada por essa homenagem, porque ela vem de um grupo de pessoas que ajudou, e está ajudando, a construir esse rico recurso que nós temos hoje aí à nossa disposição, que é a Internet, para que do Oiapoque ao Chuí se consiga usar a tecnologia para melhorar a qualidade de vida de todos nós. Eu preparei um improviso, como dizem.

[risos]

SRA. LIANE MARGARIDA ROCKENBACH TAROUCO: Porque são tantas pessoas que eu gostaria de agradecer e eu iria esquecer. Então, primeiro lugar, eu estou especialmente tocada por receber o Prêmio Alberto Courrege Gomide, porque o Gomide era um grande amigo. Eu admirava ele, a genialidade dele, ele sempre me impressionava. Quando eu ia na Fapesp, a conversa com ele era sempre surpreendente, como uma ocasião em que ele me contou que ele estava estudando matemática do caos, e eu digo: Meu Deus, o que alguém de redes vai fazer com matemática do caos? Na verdade, as redes são meio caóticas, não é? Tinha uma certa razão.

Bom, então, eu tive ajuda de muita gente, instituições, que me ajudaram a abrir caminho, e isso não é fácil, especialmente pelo fato de eu ser mulher, não é, era uma das poucas mulheres no campo das redes, tá? Normalmente, as mulheres na computação iam para áreas como análise de sistemas, não é, análise de informação, mas o meu interesse, não é, o meu desafio começou ainda quando eu estava na graduação, na Física. Eu trabalhava lá no departamento já municipal de Água e Esgoto e tinha aquelas tabuladoras IBM grandonas, não é, que eram programadas por painéis onde a gente espetava umas pegas, não é, móvel, dígito 1 do acumulador(F) para o outro, comparador, não sei o quê, não sei quanto. E aquilo me entusiasmava, eu achava aquilo

um desafio fascinante, e aprendia perguntando e enchendo a paciência do técnico da IBM cada vez que vinha ali consertar as máquinas. Aí [ininteligível] resolveu comprar um computador, selecionou, fizeram os testes lá alguns funcionários para ir fazer um curso. Eu fui selecionada, e, de novo, me apaixono por TNIT, por NCR. Fui a primeira mulher a fazer um curso de programação no estado do Rio Grande do Sul. Adorei! Dali por diante eu decidi: Bom, física é só para terminar o curso, que era a minha graduação, para ter diploma, mas eu quero mesmo é computação.

Aí fui fazendo mais uns cursos no CPD de Fortran e, quando eu me formei, casualmente, o CPD da UFRGS estava recrutando pessoas, pessoas que tinham que ser ambivalentes naquela época, faziam papel de analista e de professor, não é? A gente tanto fazia análise de sistemas e programação como e dava aula. E eu fui, então, mergulhando nessa área. Aí um tempo depois, eu já estava meio [ininteligível]: Não, eu tenho que fazer uma pós. Aí me convidaram para dar aula de Fortran lá para os ingressantes em pós-graduação em Engenharia Civil, eu: Tá bom, vou lá. Aí um ex-professor meu, Henrique Gutfrend, que foi um grande marco na minha vida também, foi meu professor de matemática, me convidou: "Ah, por que não vem aqui para um mestrado?". Falei: Mas eu na engenharia civil? O que eu vou fazer lá? "Não, não, vem, vem, nós precisamos de gente boa em programação, e tem um projeto aí complexo de método de elementos finitos, etc.". Bom, me fui, mas no ano seguinte... Terminei o curso, não fiz a dissertação, aí começou a ciência da computação em 73, aí eu: Poxa, é por aí que eu quero, não é? Aí eu comecei a fazer o curso de engenharia de computação.

Nessa época, 73, a UFRGS recebeu um *mainframe*, e esse *mainframe* tinha uma característica interessante: teleprocessamento. Uau! E o Prof. Manoel Luiz Leão era o diretor, era um homem brilhante, a quem eu tenho muito, muito a agradecer. Infelizmente, ele não está mais conosco hoje em dia. Mas ele tinha uma visão adiante fantástica, e ele investia muito: mandava os funcionários, docentes fazerem cursos em São Paulo, no Rio. Naquela época, havia empresas, como SCI, que trazia gente de fora e gente de alto nível para dar esses cursos, e um desses cursos me marcou muito. Foi em 1973, e quem ministrou o curso de *Computer Communication Networks* foi nada mais, nada menos do que o Leonard Kleinrock. Eu já conhecia ele, não é, a partir do livro dele. Ele é um guru, é um dos pais da Internet, porque foi ele que comandou a equipe que ativou a primeira ligação IMP com IMP da UCLA com Stanford, não é? Então, eu fiquei fascinada, voltei para Porto Alegre e disse para o coordenador lá do curso, Daltro José Nunes: Eu quero fazer a minha dissertação em redes. "Pois é, Liane, só tem um problema: não tem ninguém aqui para te orientar". Eu digo: Bom, dane-se, eu vou sair atrás do prejuízo, não é? E fui

conseguindo, não é, daqui, dali informações. A Embratel, na época, tinha gente muito legal em Porto Alegre, me ajudavam, normas, tudo eu conseguia com eles. A gente tinha um bom intercâmbio no plano técnico, não é, embora eu discordasse daquelas políticas meio monopolistas deles, como eu coloco no vídeo.

Bom, e eu fiz a minha dissertação, defendi, ela acabou virando um livro, e esse livro se tornou meio que um marco também, porque a Capes... Capre(F), aliás, fez um concurso, selecionou livros, o meu foi selecionado, eles mandaram, então, publicar e foi usado como livro-texto em todos os cursos de computação que na época estavam começando. Então, isso meio que popularizou, não é, um pouco mais essa área. Foi o primeiro livro, como [ininteligível], na apresentação.

Em 78, eu fui fazer uma consultoria na Universidade de Costa Rica, na área de sistemas on-line, redes, aproveitei e fui até UCLA visitar o Prof. Kleinrock, auscultando a possibilidade de fazer um doutorado com ele. Ele foi muito gentil e muito solícito e disse que sim, que poderia. Mas aí eu tive que abrir mão, porque eu fiz aquela pergunta crucial, não é, para os brasileiros que moravam lá: Como é a questão de empregada aqui? Ah! Não tem isso. Que eu tinha dois filhos pequenos na época, então tive que abrir mão, não é, do meu sonho de fazer doutorado com o Prof. Kleinrock. Continuei no Brasil pesquisando, não é?

Em 79, as universidades sempre naquele esforço de tentar ter uma rede acadêmica, então criamos o Larc. O Larc é o Laboratório Nacional de Redes. Era uma associação, não é, onde a gente tentava mobilizar o recurso, linhas, alguma coisa que pudesse fazer levar adiante a nossa ideia de conectar. Não saímos do plano teórico. Congresso sim, a gente conseguiu organizar, 83 começou a série dos simpósios brasileiros de rede de computadores. O Prof. Juergen, lá da UFRGS, coordenou o primeiro, foi lá em Porto Alegre, eu estava ajudando na organização, e em 85 finalmente eu resolvi pular para um doutorado na USP. E ali eu tive a chance de aprender com os maiores gurus da época, nossa querida Profa. Stefania Stiubiener, a minha professora de Redes, o Wilson Ruggiero, não é, também estava fazendo milagres lá com a Scopus naquela época, e eu, então, comecei a trabalhar na área de gerência de rede. Novamente, um problema: não tinha muito quem me orientasse, mas eu fui buscar apoio, não é, onde eu encontrasse. Consegui um estágio no NIC, isso foi outro marco, e a pessoa que me ajudou muito nesse sentido foi a Jake Feinler; ela foi a coordenadora do primeiro NIC, da Arpanet, no SRI, e também autora de RFCs. Ela, junto com o Postel, escreveu as primeiras normas sobre [ininteligível], como fazer, não é, organizar. Então, eu aprendi bastante... E lá era um centro onde tinha computador, assim, sobrando, não é? Imagine, em 87, foi também uma coisa muito interessante.

Bom, eu tive já um bando de alunos, 74 dissertações, 57 teses, e a minha carreira foi sempre um misto de um pouco... Um lado estava nas redes e um pouco na área acadêmica, talvez uma herança aí do meu decavô, não é, Abraham Rockenbach, que em mil seiscentos e pouco era professor na faculdade de Frankfurt. Bem eclético ele também; dava aula de grego, de ciências jurídicas, não é, mas o fascínio dele era cometas, adorava escrever livros sobre cometas. Então, em 1613 ele escreveu um dos livros. Ah, e matemática, ele era professor também de matemática.

Bom, outro, digamos assim, agradecimento que eu devo é à Sucesu, porque a Sucesu, eu participava da diretoria na década de 80, me indicou como representante do Brasil no TC6. E aí, foi o meu grande aprendizado, porque eu tive a oportunidade de conviver, tinha um representante de cada país, com os maiores gurus da história, não é? Então, por exemplo, um representante da França era o Louis Pouzin, não é, que inventou o datagrama, não é, implementou a primeira rede de pacotes no mundo; o representante da Inglaterra era o Donald Davies, que inventou o termo pacotes, não é, e depois foi para a área de segurança. Então, conviver com essas pessoas, ouvir as palestras que eles davam, porque sempre tinha um Congresso, a cada semestre, onde eles apresentavam. Era fantástico! O Ronald Uhlig, não é, que era o guru da área de *office automation* na época que o X.400 estava sendo, não é, recém-definido. Aliás, esse Congresso aqui, de 1981, foi onde eu apresentei o meu primeiro trabalho internacional, curiosamente, também impulsionado pelo Prof. Leão. O Prof. Leão... Nós tínhamos reuniões semanais, e ele sempre nos lançava desafios. Um dia, ele se vira assim para mim e uma outra colega e diz: "O instituto do futuro na Califórnia está criando um sistema de mensagens. Por que vocês não fazem alguma coisa assim?". Só olhei para minha colega assim e disse: É? Um instituto do futuro e nós aqui, não é? Tem jeito. Mas nos lançamos no desafio e começamos a trabalhar, programar, implementar, e saiu sistema de mensagens, que foi o que eu levei para esse Congresso e me abriu também portas para novas oportunidades. Outro que participava era o Bob Metcalfe, um dos coinventores da Ethernet. Então, essas pessoas estavam ali em uma mesa redonda, discutindo o que eram os rumos, o que iria acontecer. Então, foi uma oportunidade ímpar para mim conseguir a orientação que ainda no Brasil era complicado.

Lá pelo final da década de 80, então, o Demi e o Gomide conseguiram aquela façanha de trazer a Decnet para o Brasil, lá no Rio, o Alexandre Grojsgold trouxe a Bitnet, e a gente ficava ali fascinado, não é? Como é que vai ser? Como é que conseguiu? Primeiros passos foram via RENPAC, a conexão via RENPAC, bem baixa a velocidade, mas em um ano já o custo já era superior ao que a gente pagaria por uma linha dedicada na espantosa velocidade de 1.200 bits

por segundo. Mas era suficiente para os gatos pingados que usavam na época e para serviços de e-mail, não é, e outras coisinhas mais.

Em 92 foi quando a RNP fez o seu *debut*. MCT, através do CNPq, financiou um pequeno *backbone*, fez o *debut* lá em um evento da Sucesu, o Demi de novo, o Alexandre, Michel Stanton e eu fomos parte do primeiro Comitê Consultivo da RNP, não é? Aí o PoP-RS foi implantado logo a seguir, e aqui eu tenho que agradecer imensamente ao Leandro Bertholdo. O Leandro trabalhou comigo desde quando ele era bolsista de iniciação científica e sempre fez um trabalho notável, não é, e como coordenador técnico ele foi realmente uma pessoa que fez diferença no crescimento do PoP. Hoje, o César Loureiro... O Leandro foi fazer doutorado, vai estar falando aí para vocês daqui a pouco, o César Loureiro, que o substituiu, outro ex-orientando meu... Eu ponho as minhas crias sempre nos lugares estratégicos e sei o bom trabalho que eles fazem, fazem, tocam o PoP, e a Jussara Issa Musse, que era diretora do CPD na época, sempre nos deu um apoio fantástico, tenho muito a agradecer para ela, hoje é coordenadora do PoP-RS, também uma ex-orientanda.

A Rede Tchê começou logo depois, não é? Na época, o secretário de Ciência e Tecnologia era entusiasmado, e na FAPERGS nós tínhamos o Prof. Abílio Baeta Neves, que conseguiu, então, recursos para comprar os equipamentos, alugar as linhas e saiu a Rede Tchê. Aliás, o nome inicial dela não era Rede Tchê, era Rede Pampa... Repampa. Só que já estávamos com tudo pronto, já tinha até passado para o Gomide o nome do domínio para criar quando o vice-governador, que também era o secretário de Ciência e Tecnologia, em uma reunião disse: "Para, para, para tudo! Não pode ser Repampa". Repampa era o nome de um movimento separatista na época, não é, que queria tirar o Rio Grande do Sul do Brasil. Ele: "Vão me chamar de separatista". Então, troca o nome. Aí foi aquela correria toda, fala com o Gomide, desmancha o registro, e aí a gente, então, saiu com a Rede Tchê, que é um acrônimo: transmissão entre computadores heterogêneos da Internet. Então, a gente foi crescendo.

Em 93 também houve uma coisa boa, não é, que foi a compra de um Cray, supercomputador, foi o primeiro supercomputador abaixo da linha do Equador que veio para a UFRGS, e aí obrigou a implantar um *backbone*, interligando os quatro campi, pelo menos, com fibra ótica. E foi um trabalho fantástico, porque era fibra ótica que passava por postes pela rua, a gente tinha que negociar com a companhia eletrônica, depois ainda tinha uma parte que era muito longe, 17 quilômetros. Na época, a tecnologia não funcionava bem nessa distância, não é, as fibras, então botaram micro-ondas, aí tinha uma desgraceira lá das interfaces G.703 do equipamento de micro-ondas, V.35 dos roteadores, tinha que arrumar um adaptador. Aí digo: Mas onde é que vou arrumar um adaptador, meu Deus do céu? Aí tinha

uma obscura companhia, obscura crescendo, D-Link, uma tal de D-Link, eu digo: Mas que diabo é isso? Nunca ouvi falar. Isso aí é meio inseguro, não é? Aí, como era a digital que estava vendendo os roteadores, eu digo: Tá bom, vamos para roteadores. Bom, vocês têm que comprar essa interface para nós lá na Califórnia e garantir elas. Tá, então tá, então foi. Lá fomos nós, mal sabendo que a tal da D-Link ia crescer tanto, não é? Na época, eu devo um grande favor para o Demi, que foi também na época daquela inauguração da RNP, veio um lote de estações de trabalho. Eu tinha feito um projeto no CNPq e eles disseram que ok, a estação de trabalho que eu estava pedindo vinha nesse lote. E aí, estava um negócio meio enrolado, manda, não manda, aí eu: Demi, o que eu faço para receber essa estação? Aí: "Eu pago o transporte". Tá, então veio, e veio a minha Penta. A Penta é a minha filhinha querida! Desde 93 ela está no ar, até hoje. É a estação de trabalho que está no ar há mais tempo, graças ao Leandro, porque o Leandro, de vez em quando, saía a dar cursos aí pelo Brasil, e aí ele catava, canibalizava tudo que é estação para tirar peças para trazer lá para a Penta. Então, hoje tenho um estoquezinho lá. Ela já é um Frankenstein, não é? Ela tem peças daqui, dali, de acolá, mas ela nos deu condições de instalar os primeiros serviços, o Gopher, por exemplo, que era antes de ter o WWW. Quando o WWW começou, 94 mil páginas que os meus alunos do pós fizeram estão lá na Penta. Quer dizer, eram tempos bem interessantes aqueles.

Em 99, encontrei uma mensagem, não é, planejando a primeira reunião do GTER em um dos eventos da SBRC, e a gente estava lá, não é, trabalhando, participando. Embora atividade em redes estivesse bastante ativa como grupo, logo que... Na década de 80 ainda, o Gomide criou a lista, e o Demi, redes L(F), e me pediram para coordenar. E foi a primeira comunidade prática em redes que nós tivemos no Brasil. Todo mundo que tinha interesse, dúvidas, problemas discutia naquela rede. Então, informalmente, já tinha uma comunidade de redes agindo antes. Em 99, o CNPq financiou aí projetos de redes metropolitanas. Eu coordenei a Metropoa, e foi outro desafio interessante, porque era fibra apagada, espalhada na cidade, agora interligando UFRGS, PUC, [ininteligível], Procempa, companhia telefônica, ATM em cima de fibra. Em São Leopoldo, que é outra cidade, não tinha, andava outra fibra até lá, então era SSDH. Aí tinha ATN em cima de SSDH, de novo interfaces estranhas que tinha que resolver.

Então, essas experiências foram se sucedendo, e muitas pessoas foram ajudando a empurrar, não é, a nossa fronteira do conhecimento, que, obviamente, era um pouco aquém daquilo que acontecia lá fora, nos países mais ricos.

Em 2010, a RNP iniciou um novo projeto, Redes Metropolitanas. Então, nessa nova fase cresceu mais ainda a nossa rede, que até então ela estava operando, assim, meio que no vácuo, não é? Ninguém

pagava fibra, ninguém fazia nada, torcia-se que não estragasse, e não estragava. Tinha até uma coisa interessante, um *switch* ATM lá na CRT, toda a equipe foi embora que cuidava, aí o Leandro disse para eles: "Pelo amor de Deus, não toquem nisso". Então, estava em um armário chaveado, eles tinham até perdido a chave, não sabiam onde estava, e estava o Switch IBM 265, eu acho, funcionando há anos sem ninguém botar a mão nele. Não podia trocar a topografia da rede, porque não tinha como configurar aquele switch, mas seguia funcionando; PUC, UFRGS, etc., se comunicavam.

Nessa última década, eu comecei a olhar para área da Internet das coisas. Então, 2011, um projeto junto com a Unisinos, a Universidade de Caxias do Sul, foi a Remoa, Rede-Cidadã de Monitoramento do Ambiente baseado em Conceitos da Internet das Coisas. Então, sensores, realimentação, um outro mundo de redes começou. Em 2015, mundos virtuais, imersivos, não é, também o 3D, para criar laboratórios virtuais, para resolver um problema que hoje a gente ainda tem no Brasil. Em 2017, eu criei o projeto Alerta. Aí era a ideia de ter um ambiente lógico de encaminhamento, resposta e tratamento de avisos, e sentisse coisas no campus, não é, e avisasse, além de contar com a participação dos usuários para avisar anormalidades, não é? Então, a gente combinava o usuário como sensor inteligente com sensores de temperatura, pluviométricos, CO2, nível de CO2, que quando excedidos também poderiam ser avisados... Ultravioleta também pelos sensores, para avisar, especialmente os mais branquinhos aí do Sul, que na hora do meio-dia eles não podem ficar mais de 15 minutos no sol, não é?

Então, nessa linha de Internet das coisas, nós começamos a ir um pouquinho mais adiante, tentar pendurar as pessoas, ou ler a mente das pessoas. Então, começamos a testar o NeuroSky, MindWave, um artefato que ficava aqui, não é, e ele mede a intensidade da atividade cerebral. Então, a gente pode avaliar quando a pessoa está prestando atenção, não está. Fizemos algumas coisas com pedômetros, transmitindo para celular, para ver atividade física, medidores de batimento cardíaco. A gente está começando a ver como é que é ter outros tipos de equipamentos na rede. Até eu on-line! Esse camaradinha aqui, não é, entra em Bluetooth e pode ser lido e configurado pela médica, não é? Eu tenho aqui dentro.

Então, essas são as atividades, não é, que atualmente eu estou envolvida, e muito grata, não é, aos meus alunos do doutorado lá na computação, que eu me afastei já faz um bom tempo, estou mais na informática e na educação agora, e me são, digamos assim, a mão de obra preciosa que eu posso usar para tentar colocar em prática algumas ideias.

Bom, então esse foi um breve relato, espero que breve mesmo, às vezes eu me entusiasmo falando, de como é que eu cheguei nesse ponto agora, não é? E os amigos do GTER, do GTS foram também preciosos, porque sempre participar desses eventos é uma fonte de aprendizagem perpétua, e esse é o bom da área de redes, não é, gente? A gente acha que sabe tudo, mas não sabe. Sempre tem um *bug* escondido correndo atrás de alguma nuvem, algum equipamento que a gente tem que perseguir, porque nunca viu aquele tipo de anormalidade antes. Então, mais uma vez, obrigada, obrigado pelas lindas flores, não é? Hoje de manhã fiquei encantada recebendo essas flores aqui em casa, e era isso que eu tinha a comentar.

SR. FREDERICO NEVES: Alexandre?

SR. ALEXANDRE GROJSGOLD: [interrupção no áudio].

SR. FREDERICO NEVES: Você está no *mute*, Alexandre.

SR. ALEXANDRE GROJSGOLD: Olá, bom dia a todos. É um grande prazer para mim estar aqui nessa homenagem à Profa. Liane Tarouco. Eu fiquei, na verdade, muito contente e um pouco surpreso, me sinto muito honrado de ter sido chamado para falar nessa homenagem.

A primeira vez que eu ouvi o nome de Liane Tarouco foi lá no finalzinho dos anos 70. Eu estava fazendo as cadeiras de mestrado na COPPE/UFRJ já nessa área de rede de computadores, que, na época, como Liane disse, atendia pelo nome de teleprocessamento, não é? Eu sofria muito, uma dificuldade muito grande de ter literatura sobre o assunto, tinham poucos livros importados, não é, em geral difíceis de serem obtidos. É claro, naquela época não tinha web, não tinha Google, era muito difícil você conseguir qualquer informação, não é? Até aquele livro clássico, todo mundo conheceu depois, do Tanenbaum, só ia aparecer nos anos 80. Então, livros, então, com uma abordagem mais prática dizendo como eram as coisas, como se fazia, como funcionava eram muito raros. Tinha alguns livros que vinham lá dos Estados Unidos de um tal de James Martin, que a Liane certamente lembrará dele.

SRA. LIANE MARGARIDA ROCKENBACH TAROUCO: Fiz curso com ele.

SR. ALEXANDRE GROJSGOLD: É. Eu procurava nas bibliotecas, e depois o James Martin ficou riquíssimo e comprou uma ilha nas Bahamas, onde ele viveu o resto da vida fazendo palestra nas Bahamas. Eu acho que Liane certamente não chegou nem perto nesse quesito.

Bom, eu mesmo, como parte do curso de mestrado, tinha escrito um resumo sobre redes, sobre redes locais no caso, sistematizando alguns temas e tal, deu um apostilão, pensei em publicar, coisa que eu

nunca fiz, e quando vi o livro da Liane eu confesso que fiquei com um pouco de inveja, não é? Eu falei: Puxa vida, quem é essa professora do Rio Grande do Sul que escreveu um livro? Foi realmente o primeiro livro em português e, na verdade, o primeiro livro que trazia informações práticas que antes não se encontrava em lugar nenhum. Fiquei com aquela ponta de admiração. Depois, passei um tempo longe do Brasil, passei um tempo no exterior, estive na França e não ouvi mais falar no nome da Liane Tarouco até eu voltar ao Brasil, e aí nos meados dos anos 80, eu comecei a me envolver com iniciativa de formação de redes acadêmicas, tanto aqui no estado do Rio de Janeiro como no Brasil inteiro. Essas iniciativas acabaram desaguando na formação da Rede Nacional de Pesquisa, da RNP, mais ou menos em 1992, e foi aí que eu voltei a ter contato com o nome Liane Tarouco, que eu lembrei: Ah, é aquela professora daquele primeiro livro que estava liderando iniciativas de rede lá naquele estado mais ao sul do Brasil e estava promovendo formação de redes na sua região, e que participava ativamente dos esforços para montagem da rede nacional.

Eu queria... A Profa. Liane já falou, mas eu queria reiterar essa ideia, que aqueles eram tempos muito difíceis para esse tipo de atividade, não é? Havia um desafio tecnológico, é claro, tinha uma curva de aprendizado, era uma tecnologia nova que a gente tinha que aprender, mas a parte mais complicada, talvez, foi o desafio político, o desafio cultural, se eu posso dizer assim, não é? A gente tem que lembrar que em 84, eu acho importante sempre relembrar isso, sobretudo para o pessoal mais novo, que não viveu aquela época, de 84 a 92 a gente estava sob as fortes restrições da reserva de mercado. Quer dizer que toda a aquisição de software, até de hardware também, era muito complicada, estava sujeita à regulamentação por parte da famosa SEI, Secretaria Especial de Informática, sobretudo para sistemas pequenos, não é, porque a reserva dizia respeito justamente a pequenos sistemas, minicomputadores, como chamava na época. Então, tudo era muito difícil de obter. Por outro lado, as telecomunicações já eram monopólio do estado já desde a criação do mundo e fortemente regulamentadas. Então, foi assim, não é? A Telebras, através de seu braço operacional, Embratel, criava regras extremamente restritas e, na verdade, eles fizeram de tudo, tudo o que podiam para retardar iniciativas, como da rede acadêmica, como de uma rede aberta, e que pudesse ameaçar de alguma forma o monopólio, não é, os interesses das estatais de telecomunicações.

Então, eu fiz questão de reiterar essas coisas para ressaltar o valor e a importância que a Liane teve naquele momento, não é? Quem conhece a Profa. Liane sabe da sua personalidade forte, sabe do seu caráter extremamente determinado e objetivo nas suas falas e nas suas apresentações. A Liane é aquela pessoa do tipo que não desanima face a obstáculos, que trilha o caminho até atingir os objetivos, que

lidera e bota as coisas para acontecer. Além do manifesto conhecimento que ela tem do assunto, não é, muitos anos trabalhando e estudando, Liane foi uma voz fundamental nessa fase da rede, seu jeito muito objetivo de dizer as coisas e pelo pragmatismo também. Desde aquela época, a Liane sempre esteve presente em todos os momentos de desenvolvimento da rede acadêmica brasileira, reuniões, apresentações, ela sempre presente em praticamente todas elas, em comitês, etc. Eu mesmo, que atuei por muitos anos da RNP, várias vezes estive junto com Liane em congressos aí pelo mundo afora, também reuniões no Brasil quando tive oportunidade de conhecê-la mais de perto, não é, deixou de ser apenas um nome, uma autora, e passou a ser uma pessoa que eu conheci mais de perto, e aprendi a admirar aquela pessoa objetiva, determinada, comprometida, de uma tremenda resiliência, que sabe enfrentar as diversidades e que foi capaz de reconstruir tudo o que havia a ser reconstruído ao final de cada tempestade.

Encerrando: Pela participação na verdadeira briga que foi a abertura da Internet no Brasil, foi uma briga terrível, pelo trabalho que ela desenvolveu de divulgação do tema de rede de computadores e também por sua atuação como professora, obviamente, Liana é totalmente merecedora de todo reconhecimento e, mais especialmente, de um prêmio que leva o nome de Alberto Gomide.

Aqui só uma palavrinha: Alberto Gomide, outra pessoa que muito batalhou naqueles tempos, que eu conheci pessoalmente, tive o prazer de conhecer pessoalmente e que encontrei em várias ocasiões, e fico só pensando o que diria o Gomide hoje com aquele seu jeito irônico, agora, ao ver seu nome escrito em um troféu. Eu só lamento que ele não possa estar aqui para participar também dessa homenagem. Muito obrigado, um grande abraço, Liane.

SRA. LIANE MARGARIDA ROCKENBACH TAROUCO: Obrigada, Alexandre.

SR. FREDERICO NEVES: Muito obrigado a todos. Com isso, a gente encerra o Prêmio Alberto Courrege Gomide edição 2020. E lembrando ao pessoal que nos está assistindo remotamente, como sempre, todo o material do GTER está sempre disponível no servidor FTP, ftp.registro.br/pub/gtr/gtr49. E a pedidos aqui, eu gostaria que a gente mudasse a tela para um outro formato aqui, para que a gente pudesse aplaudir, não é, finalmente a Profa. Liane e os nossos participantes nesse Prêmio Alberto Courrege Gomide 2020. Por favor.

[aplausos]

ORADOR NÃO IDENTIFICADO: Abre o microfone, pessoal!

[risos]

[aplausos]

SR. FREDERICO NEVES: Muito bem. Então, agora, para a nossa próxima apresentação, de novo, para quem está remotamente, o material já está no servidor FTP, mas, como todos estamos remotos, a apresentação vai ser transmitida diretamente pelo YouTube. Eu gostaria de chamar o Michel Machado da Digirati Hostnet, que vai nos falar um pouquinho sobre o "Gatekeeper - primeiro sistema de proteção DDoS *OpenSource*". Michel, por favor.

SR. MICHEL MACHADO: Ok. Bom dia. Vocês conseguem me ouvir? Ótimo. Muito obrigado pela introdução, Frederico. Bom dia a todos. Eu vou aqui compartilhar a minha tela para mostrar os slides que eu tenho. Ok. Bem, funcionou. Vamos lá!

Em 2009, 2013 e 2015, a Hostnet sofreu grandes ataques DDoS que deixaram todos os nossos sistemas indisponíveis. Esse tipo de experiência dolorosa causou problema em toda a empresa, não... Assim, todo mundo foi afetado, nossos clientes, os clientes dos nossos clientes, e esse tipo de experiência quando a gente passa, a gente fica sempre com a impressão de que foi algo isolado, que nós somos os únicos passando por esse tipo de coisa, mas segundo as pesquisas anuais da Arbor Networks, ataques de DDoS são considerados a principal ameaça operacional entre as entidades que são entrevistadas aqui, inclui agências do governo, *cloud providers*, empresas normais, que não têm nada a ver necessariamente com Internet o negócio principal. E essa pesquisa mostra a amplitude a que os ataques de DDoS já são hoje, mas tem dois aspectos dos ataques de DDoS que ajudam a entender porque há essa preocupação coletiva com eles: o primeiro aspecto é capacidade de pico e o segundo é a complexidade dos ataques.

Esse gráfico, que foi recentemente publicado pelo Google, deixa claro a capacidade de pico dos ataques de DDoS, pois eles têm crescido na última década exponencialmente, e isso é demonstrado sobre três métricas: a métrica de banda, pacotes e requisições por segundo. E esse crescimento exponencial significa que nenhuma entidade está imune a esse problema, e mesmo empresas que não são alvo desses ataques não podem se sentir, eu não diria protegida, mas imune a eles por causa que existem os efeitos colaterais. Um exemplo público aconteceu em 2016, quando a empresa Dyn recebeu um grande ataque e que usuários nos Estados Unidos e Europa ficaram sem acesso à Internet.

O crescimento aos ataques de DDoS continua mesmo em um ano tumultuado como em 2020. Em junho, tivemos o maior ataque segundo a métrica pacotes por segundo, com 809 milhões de pacotes por segundo, um crescimento de 24% sobre o recorde anterior, que foi registrado ano passado, e dois outros ataques chegaram a 90% da capacidade dos recordes anteriores, um contra a AWS, que chegou a

2.3 terabits, enquanto o recorde foi de... Ou melhor, o recorde atual(F) é de 2.54 terabits, e a Cloudflare chegou bem próximo do ataque da Akamai.

Embora a capacidade de pico dos ataques nos ajuda a dimensionar a capacidade do sistema de proteção necessário, esses aspectos dos ataques de DDoS não oferecem uma orientação, uma pista de como a gente deve evoluir os sistemas. Para poder entender... Para poder nos orientar e nos preparar com a evolução do sistema, a gente precisa entender a complexidade dos ataques atuais, e segundo relatórios reportados por vários membros da indústria, cerca de 90% dos ataques atuais apresenta um nível de sofisticação modesto.

Esse *paper*, *The Catch-22 Attack*, que foi publicado ano passado, aponta que se os ataques atuais evoluírem para explorar a limitação do número de filtros simultâneos que as proteções atuais suportam, esse sistema de proteção não vai conseguir segurar esses ataques, ainda que a capacidade desses ataques seja inferior à capacidade que o sistema consegue atender. Isso é preocupante, porque diferente de *papers* como *Coremelt* e *Crossfire*, que são dois ataques bem sofisticados, o ataque que é documentado nesse *paper*, *Catch-22*, é um ataque bem mais simples de ser implementado. Para entender de forma intuitiva o que eu quero dizer com esse limite no número de filtro simultâneo, você pode considerar que se você tentar configurar um *Firewall* ou qualquer mecanismo de filtro de rede para limitar banda por classes de tráfego, o número de classes que você vai conseguir limitar vai estar, no melhor dos casos, na casa de milhares, mas você não vai conseguir, por exemplo, ter um limite de banda por fluxo, *flow*, por conta da forma como esses mecanismos são projetados. Eles têm uma capacidade proporcionalmente limitada comparado com os ataques a... O que os atacantes podem fazer.

No caso de gatekeeper, não somente é possível fazer uma limitação de banda por fluxo como, na verdade, a gente encontrou que, na prática, ter dois limites de banda por fluxo oferece um mecanismo de proteção eficiente em produção. Outra característica do gatekeeper é escalar para qualquer capacidade de pico. *Mail.ru*, um portal russo, web russo, e o primeiro usuário do gatekeeper que não teve qualquer vínculo direto com o nosso grupo, está trabalhando atualmente na instalação de um gatekeeper de 1 terabit, e o que motivou o *Mail.ru* a experimentar e adotar o *gatekeeping* foi a velocidade de mitigação dos ataques.

Segundo a empresa Kaspersky, que é uma empresa de segurança russa, mais de 80% dos ataques que registraram no último ano duraram menos de quatro minutos. Então, não há tempo para intervenção humana, e mesmo os sistemas que procuram por assinatura de pacotes para poder tentar filtrar não são efetivos por

causa que eles costumam levar mais de um minuto ou dois para conseguir as assinaturas, até o tempo de os filtros se propagarem na rede, eles não são suficientes para... Quando a sequência de ataques é muito curta.

No restante dessa apresentação, eu vou explicar como é que o gatekeeper funciona, como é que se escreve uma política de rede, apresentando um modelo simples para ajudar nesse processo, a política de rede é elemento-chave em qualquer instalação do gatekeeper, e tentar botar todos esses componentes juntos, mostrando como é que o sistema se comporta em uma SYN Flood, e a ideia é concluir mostrando o que seria o final de jogo para os atacantes e o que a gente prevê com uma evolução para o gatekeeper no médio e curto prazo.

O primeiro aspecto para entender gatekeeper é onde os servidores gatekeeper devem ser instalados. Os servidores gatekeeper devem ser instalados em localidade geograficamente distribuída e com grande capacidade de troca de tráfego, e esse tipo de localidade nós chamamos de *vantage points*. As características mínimas que são esperadas são: capacidade computacional para serem instalados os servidores gatekeeper; a banda de entrada tem que ser barata, porque é onde o sistema vai descartar o tráfego de abuso; essas localidades têm que suportar o anúncio de prefixo de rede pelo BGP, porque essa vai ser a forma que a gente vai atrair o tráfego, que a gente vai, na verdade, montar uma rede Anycast; e o quarto item são links privados que ligam os *vantage points* ao Data Center que está sendo protegido. No ataque, pode haver vários Data Centers e eles podem estar fisicamente distantes um dos outros, mas nessa apresentação eu assumo que há apenas um Data Center que está sendo protegido, mais para poder simplificar a exposição.

Exemplos desses *vantage points* seriam os PTTs no Brasil, link de troca de tráfego que existe unilateral entre as empresas e alguns dos provedores cloud pelo mundo também suportariam também ser *vantage points*. O principal motivo que provedores cloud hoje são desclassificados, não podem ser usados como *vantage points* é o fato de eles não suportarem anúncio BGP, mas existe um número de provedores cloud pelo mundo que poderiam atender como *vantage points*.

Uma vez escolhidos os *vantage points*, os gatekeepers podem ser instalados. Nesse diagrama aqui, a região sombreada com azul é tudo que pertence a quem está instalando o gatekeeper. E, agora, vamos tentar, nos próximos slides, entender como é que o fluxo é estabelecido no gatekeeper. E outra coisa importante é que daqui para frente sempre quando eu me refiro a fluxo, ou talvez eu fale *flow*, ele vai ser definido pelo seguinte par: endereço de origem-endereço de

destino. Ou seja, não inclui qualquer informação relacionada ao protocolo de transporte, seja TCP, UDP ou qualquer outro.

Pois bem. Quando o cliente envia tráfego para o Autonomous System protegido pelo gatekeeper, os pacotes são entregues ao *vantage point* mais próximo ao cliente, isso ocorre por conta do anúncio BGP, e servidores gatekeeper são tipicamente balanceados no *vantage point* onde eles são instalados ou pelo roteamento ECMP, *Equal Cost Multipath*, mas qualquer mecanismo que distribua tráfego respeitando como é que o fluxo é definido seja suficiente.

Quando o pacote chega a um servidor gatekeeper, há duas ações possíveis: uma para fluxos que já foram estabelecidos e outra para fluxos novos. Os fluxos estabelecidos, eles já têm um programa BPF associado, então o que quer que... O que vai acontecer com esses pacotes desse fluxo depende unicamente sobre esse programa BPF, que a gente vai ver em mais detalhes depois na apresentação, mas ações típicas seriam limitar banda, classificar e punir abusos. Se os pacotes nesse *flow* são autorizados a passar, esses são enviados ao seu destino pelo link privado, ou pela Internet pública. Isso é o que garante que não... Depois que você passa pelo gatekeeper não há como o atacante tentar ignorar o sistema e tentar atacar a sua rede indiretamente.

Quando um fluxo novo é identificado, os pacotes desse fluxo são encapsulados e enviados para os servidores grantor, que são localizados no Data Center protegido. A função dos servidores grantor é associar um programa BPF a cada fluxo. Como essa associação é feita e descrita por um *script* Lua, o qual chamamos de Lua *policy*, o servidor gatekeeper é notificado da decisão do servidor grantor e o *flow* é considerado estabelecido. O pacote devidamente capsulado é enviado ao servidor de destino.

Agora, só um sumário rápido para rever o que a gente acabou de apresentar nessa sequência de slides: os pacotes de um cliente são entregues ao *vantage point* mais próximo; os servidores gatekeeper encapsulam e enviam o pacote de *flows* novos aos servidor grantor ou executam programa BPF associado aos fluxos para decidir o que fazer com os pacotes; servidores grantor associam um programa BPF a cada *flow* novo; servidores grantor notificam servidores gatekeeper das decisões da política de rede; e, finalmente, os servidores gatekeeper aplicam as decisões da política de rede através dos programas BPF.

Agora que temos uma visão geral de como o gatekeeper funciona, fica claro que o comportamento inteiro do sistema é definido pela política de redes, e é por isso que esse é um elemento tão importante em qualquer instalação de gatekeeper, e esse é o tópico dessa nova seção da apresentação.

A política de rede, ela é formada de dois componentes: os programas BPF, que vão rodar no gatekeeper, e a Lua *policy*, que [ininteligível] grantor.

Para que a gente possa escrever essa *policy* de rede, a gente estabeleceu três passos para orientar quem está fazendo isso pela primeira vez, e o primeiro passo é identificar os perfis de rede. Um perfil de rede, ele pode ser aplicado a um único servidor, a um grupo de servidores ou a um prefixo de rede, um bloco de endereço IPs. Um exemplo de perfil de rede seria servidores de envios de e-mail, esses servidores não têm a *listening sockets*, eles só acessam servidores externos pela Porta 25, pelo protocolo SMTP, recebe muito pouco tráfego externo, comparado ao que eles enviam e as informações necessárias para poder descrever um perfil são tipicamente encontradas em arquivos de configuração. O próprio servidor de produção pode ser investigado para oferecer as informações e a documentação interna disponível para quem [ininteligível] quem instalou os servidores.

Uma vez que todos os perfis de rede são identificados e descritos, a gente pode passar para o segundo passo que é essencialmente converter esses perfis de rede em programas BPFs. Cada programa BPF deve classificar os pacotes de um fluxo associado entre... em três classes: a primária, a secundária e a indesejada. A classe primária representa o objetivo do perfil de rede. Por exemplo, nos servidores de envio de e-mail, são os pacotes enviados aos servidores externos, com os e-mails, obviamente. A classe secundária inclui tráfego que é necessário ou tolerado, mas que só deveria estar presente como uma pequena fração da classe primária. Normalmente, de 20%, ou menos, do tráfego da classe primária. E um exemplo desse tipo de tráfego seria pacote SYN, do TCP, ou mensagens ICMP. E a classe indesejada são [ininteligível] tráfego que não faz sentido. Por exemplo, em um servidor de e-mail, de envio de e-mail, tráfego UDP, ou receber conexões, não faz sentido, e ele pode ser... esse tipo de pacote pode ser descartado imediatamente.

Além de classificar os pacotes, um programa BPF impõe dois limites de banda: o limite primário, o qual é aplicado antes da classificação dos pacotes e o limite secundário, o qual é aplicado depois da classificação dos pacotes. Memorizar essa ordem em que os limites de banda são aplicados, vai ajudar a gente entender quando for dar o exemplo de uma SYN Flood.

Agora que a gente já tem todos os programas BPF, a gente pode passar para o terceiro e último passo para produzir uma política de rede. E o terceiro passo é escrever a Lua *policy*. Lembrando que o objetivo da Lua *policy* é associar um programa BPF para cada fluxo novo. Essa informação de como associar(F), você já gerou como um

subproduto do primeiro passo. Por exemplo, quando você disse: Ah, eu quero escrever um perfil de rede para os servidores de envio de e-mail. Você, nesse momento, já vai ter que identificar quais são os servidores de e-mail. Aí no caso aqui eu dei como exemplo que todos os endereços 10.99.99.128/25 são servidores de envio de e-mail. Então você já tem esse mapeamento. Você só vai botar isso na Lua *policy*.

Escrever uma política de rede é essencialmente programar, para você gerar um programa BPF ou gerar em código Lua. Mas a gente tem modelos para fazer os dois. E muito do esforço é basicamente converter a descrição em texto, de um perfil de rede para o programa, copiando a partir desses exemplos.

E, finalmente, a gente tem... Até aqui você já... quando você completar o terceiro passo nesse estágio aqui, você já tem uma *policy* de rede completa. Mas a gente encontrou, na prática, que existe um melhoramento que você pode fazer na Lua *policy*, que é relativamente simples, que é classificar o endereço de origem. Existem várias listas de prefixo de rede para classificar, por exemplo, bogon, *abusers* e malware. Esse tipo de origem, você pode bloquear. Não existe qualquer sentido em você deixar passar. Porque só vai lhe causar problema. Você pode fazer ajuste do limite de banda, baseado, se quem está se conectando a você é seu parceiro. Dependendo do país de origem, se você não estiver disponível, se vem de um usuário final e não de um servidor.

E também você pode identificar o tipo de atividade que aquela origem está fazendo. Existem classificações para CDN, provedores clouds, *crawler*. E você, obviamente, pode identificar os seus escritórios, e isso permite você a enviar programas BPF diferentes, dando mais ou menos acesso àquele tipo de serviço, àquele tipo de atividade. E quando... Se você decidiu adicionar isso à sua Lua *policy*, você vai precisar baixar essas listas, manter elas atualizadas e resolver conflitos entre elas, de endereço IP ou de prefixos inteiros. Existe essa ferramenta, desenvolvida pelo Andre Nathan, o que é um outro membro do nosso projeto, que desenvolveu, né, também é *open source* e que ajuda a fazer tudo isso de uma única vez.

Ok. São... A gente descreveu vários componentes. É comum ficar um pouco confuso, se você está vendo isso pela primeira vez. Só que a minha intenção agora é tentar mostrar como o gatekeeper se comporta durante SYN Flood com a esperança de ajudar você a entender como esses componentes interagem. E se você conseguir entender esse exemplo, você provavelmente vai conseguir deduzir o comportamento do sistema sob outras condições. O motivo por que eu escolhi o SYN Flood, porque segundo a Kaspersky, quase 85% dos ataques no último ano são dessa natureza. Ok.

Para entender o meu exemplo, eu fiz algumas *assumptions,* mais na intenção de simplificar exposições. Elas podem ser generalizadas, mas ficaria mais complicado de explicar o que vai acontecendo. E a primeira é que as máquinas que são [ininteligível] pelo atacante mandam toda a capacidade dela de links de SYN Floods. Os programas associados... Os programas BPF vão ser associados aos fluxos, como foi descrito anteriormente. E notar que de acordo com a política de rede que definimos na seção anterior, pacotes SYN contam com um tráfego secundário. Isso vai ser importante quando eu começar a mostrar os gráficos. Portanto, cada fluxo limitará seus pacotes SYN com limite secundário. Ok. Isso é só um detalhe, mas vai ficar claro nos gráficos.

Aqui, nesse exemplo, a gente tem o tráfego de um único fluxo, você pode generalizar pelos outros, mas se você(F) quiser olhar um único fluxo por vez, em que ele inicia, não importa bem a banda que ele inicia, mas ele sobe até atingir a capacidade máxima do link de onde ele está usando para usar como ataque. E a gente tem aí o limite secundário. Essa barra deixa claro que o limite secundário é constante. E ele é definido pela Lua *policy* no momento em que o programa BPF é associado a um dado *flow*. E isso vai ser diferente do limite primário, pois ele não vai ser constante. A gente vai ver como é que ele funciona agora.

O limite primário, na verdade, ele tem um limite máximo. E esse limite máximo é definido pela Lua *policy* no momento em que o programa BPF é associado a um fluxo. O limite primário inicia no seu máximo, mas ele ainda é incrementado quando o tráfego do *flow* é maior que o seu máximo. Ou seja, você limitou a banda a 10 megabits, e se o cliente passar desse limite, ou seja, não respeitar a perda de pacote, como o TCP respeitaria, tentaria trabalharia em volta desses 10 megabits, esse limite vai começar a ser decrementado. Se o limite primário cair tanto que ele alcance o limite secundário, todo o tráfego vai ser alimentado(F) pelo limite primário. Porque o limite primário, se você lembrar, ele é testado antes da classificação dos pacotes. E, finalmente, se o limite primário continuar caindo e chegar a ser negativo, ele, nenhum pacote vai poder passar.

Agora, vamos botar isso em um gráfico. Você vê que o limite primário começa no seu máximo e ele só vai começar a cair quando o tráfego de ataque passa esse limite, esse máximo. E a partir daí ele continua caindo. No meu caso, ele continua caindo indefinidamente, porque o ataque continua, constante.

E aqui a gente tem o que realmente passa do tráfego... o vermelho é o que o atacante está mandando, e o azul é o que o servidor gatekeeper deixa passar. O motivo é porque apenas... A gente começa já no limite secundário, porque os pacotes são do tipo SYN. E quando

o limite primário alcança o limite secundário, ele começa a reduzir mais ainda o que deixa passar. Quando o limite primário chega a ficar negativo, nenhum tráfego passa daquele fluxo.

Resta responder à pergunta de quando é que esse fluxo terá algum pacote aceito novamente. E há apenas duas situações quando é que isso volta a acontecer. O primeiro é quando o tráfego do fluxo cair abaixo do máximo do limite primário e houver tempo suficiente para o limite primário ficar positivo. Ou seja, o quão negativo o limite primário ficar, vai ser uma punição e ela vai ser proporcional ao abuso. A outra possibilidade, é o registro daquele fluxo expirar, do servidor gatekeeper, e aí o que acontecer primeiro é o que vai permitir aquele mesmo fluxo poder ter pacotes aceitos novamente.

Ok. A gente tem agora o entendimento geral do gatekeeper. Mas falta agora a gente discutir... esquecer um pouco os detalhes e tentar pensar em mais alto nível o que vai acontecer no sistema quando os ataques começarem a evoluir. Porque não adianta você escrever uma política efetiva agora, os ataques evoluem, e você não está preparado para aquilo. Então, inevitavelmente, você vai ter que evoluir a política de rede para poder acompanhar a evolução dos ataques. Aqui eu mostro três exemplos. O primeiro, que é você... um mecanismo para evitar *anti-spoofing*. Você instala um sistema de banco de dados distribuído e registra esse banco de dados, o *vantage point* e o endereço de origem, para poder saber qual é o local de entrada regular, normal daquela origem. E se essa origem mudar de um *vantage point*, por exemplo, uma universidade brasileira aparecer no tráfego na Europa, você pode identificar isso como *spoofing*.

Existem certas limitações, e você tem que lidar com as situações de perda de um *vantage point* ou a mudança deles, mas isso também é uma técnica que dá para você identificar *anti-spoofing*. Você pode obter informações da aplicação que está sendo protegida, existe esse *plugin server security*, do WordPress, que gera vários tipos desse tipo de *abuser*, que pode... os dados podem ser exportados e alimentados para a política de rede. Ou você pode usar um sistema de detecção de intruso para gerar assinatura de pacotes ou outras informações que você pode alimentar a política, que pode, inclusive, influenciar os programas BPF que são gerados.

Mas fica a pergunta de: quando é que acaba esse jogo entre cão e gato? Ou gato e rato? Qual o final de jogo para o atacante? Para onde é que está indo com isso tudo? Para entender para onde é que a gente está indo, a gente tem que entender esse conceito de final de jogo para o atacante. O final de jogo, ele ocorre quando o custo para identificar o tráfego de ataque é maior ou igual ao custo de servir esse tráfego. De uma forma, talvez, mais simples, é quando não é mais possível ou viável identificar o tráfego de ataque.

Atualmente, essa atuação já acontece com LDNS(F) sobre o DP. Isso deve mudar, à medida em que essa migração, agora, DNS para TCP. Ou seja, atualmente, quem tem uma instalação DNS de grande porte vai ter que pensar em algum mecanismo não trivial para a proteção, porque agora o custo de servir é mais alto. Mas quando você está no final de jogo, a melhor ação que você pode ter é servir todo o tráfego. Porém, na prática, quando a rede entra em situações de estresse, principalmente em um ataque de DDoS de grande porte. Acontece que a porcentagem de clientes que você pode atender é muito, muito pequena. Mesmo ignorando o ataque. Porque a rede não tem nenhum mecanismo de coordenação e isso gera vários colapsos e perda de pacotes, que causa uma confusão na rede.

A gente pretende, eventualmente, adicionar no gatekeeper essa *feature* que a gente chama de *flow orchestration*. Que basicamente você cria uma fila com todos os fluxos, você só atende o começo da fila, a ideia é aproximar isso para a quantidade máxima de clientes que você consegue atender. E esses clientes têm um período em que eles têm que ser atendidos, por exemplo, dez minutos, eles têm que fazer o que o seu site oferece, o seu serviço oferece, e depois daquele período, eles são alocados no final da fila e a fila vai movendo. Isso não acaba o ataque. Porque vai ter gente esperando por longos períodos para poder ser atendido. Mas, pelo menos, seu sistema sempre vai estar operando na capacidade máxima, atendendo o número máximo de usuários que ele pode.

O que a gente prevê adicionar ao gatekeeper é: suportar placas de rede de 100 gigabits na velocidade máxima. E isso ajuda a baratear instalações de gatekeeper. Adicionar a funcionalidade de *load balancing* nas políticas. Então, quem... em uma instalação de gate(F) que vai ser mais útil, porque você não precisará ter *load balancing*, e adicionar *flow orchestration*, que seria um seguro para os dias de chuva.

Bem, sei que eu cobri bastante itens aqui, vou tentar sumarizar em apenas alguns itens. Gatekeeper entrega uma proteção contra ataque DDoS sem paralelo(F) nas soluções atuais. A mitigação dos ataques ocorre em segundos após o início do ataque. Gatekeeper escala para qualquer capacidade de pico, é *open source* e pronto instalação e produção e o valor entregue por uma instalação de gatekeeper vai aumentar à medida que os novos recursos já planejados serão incorporados.

Você pode usar esse QR Code para chegar no nosso link(F), aprender mais sobre gatekeeper. Muito obrigado. E estou aberto a perguntas.

SR. RUBENS KUHL: Obrigado, Michel. A primeira pergunta que a gente tem é do Cristian Cardoso, ele perguntou se os servidores são *bare-metal* ou virtualizados?

SR. MICHEL MACHADO: A gente dá preferência por *bare-metal*. Mais porque o código tira vantagem de várias otimizações de hardware, que nem sempre estão disponíveis nos servidores virtualizados. Mas é possível, sim, rodar o gatekeeper em um servidor virtualizado.

SR. RUBENS KUHL: Então, de perguntas que a gente tinha on-line era isso. Obrigado, pessoal. Obrigado, Michel.

SR. MICHEL MACHADO: Obrigado.

SR. FREDERICO NEVES: Muito bem, pessoal. Com isso, a gente termina a segunda apresentação do GTER 49. E nós vamos dar uma pausa agora para um break. Voltamos às 10h40. Relembrando: GTER 49, evento do Grupo de Trabalho em Engenharia de Redes do Comitê Gestor da Internet no Brasil. O material do evento se encontra no servidor FTP do registro, ftp.registro.br/pub/gter/gter49. Então, nos vemos em 20 minutos.

[intervalo]

SR. FREDERICO NEVES: Olá, pessoal. Muito bem-vindos, novamente, ao GTER 49. E lembrando, o GTER 49, inserido na 1ª Semana de Infraestrutura da Internet no Brasil. Hoje é o primeiro dia, o evento vai até sexta-feira. Amanhã nós teremos o GTS e quarta, quinta e sexta o IX Fórum.

Para dar continuidade agora ao evento, nós vamos ter o Bruno Bioni da Data Privacy Brasil, falando um pouquinho para a gente sobre LGPD. O que muda no gerenciamento de incidentes de segurança. Bruno, por favor.

SR. BRUNO BIONI: Bom, primeiramente bom dia a todos e todas. Eu queria agradecer muito o convite, na pessoa do Fred, do Rubens, Klaus, Cris. Enfim, são amigos, não é? Eu tive a oportunidade de trabalhar no NIC.br, então, é sempre bom estar de volta nesse espaço que é superprivilegiado para a gente poder fazer discussões e especificamente sobre o tema da qual eu tenho trabalhado aí durante os últimos anos, que é sobre produção de dados pessoais.

Então, o que a gente pensou hoje, conversando, inclusive, com os organizadores e as organizadoras do evento foi fazer uma fala na qual a gente pudesse olhar um pouquinho para o cenário posto pela Lei Geral de Proteção de Dados Pessoais. E, da mesma forma, a gente pudesse fazer uma ponte entre essas duas, digamos assim, comunidades. A comunidade do campo de proteção de dados pessoais

e a comunidade do lado de incidentes de segurança, segurança de redes, assim por diante.

Então, o meu objetivo aqui principal é entender como é que a Lei Geral de Proteção de Dados Pessoais, ela dá um caldo ainda maior para toda a estrutura, né, a gestão de um incidente de segurança. E aí é buscar, olhar para a Lei Geral de Proteção de Dados Pessoais a partir de dois eixos principais, não é? Então, a nossa conversa, ela vai ser dividida da seguinte forma. Primeiro, é olhar para a Lei Geral de Proteção de Dados Pessoais enquanto uma janela de oportunidade. Ou seja, a Lei Geral de Proteção de Dados Pessoais, ela pode ser uma amiga e não uma inimiga do pessoal que está trabalhando com segurança de redes? E aí eu vou tentar plantar essa semente aqui junto com vocês.

E, em um segundo momento, entender como é que a Lei Geral de Proteção de Dados Pessoais, ela cria novas fronteiras para o gerenciamento de incidente de segurança e o que ela muda hoje no cenário regulatório, não é? Então, responder perguntas como: existe um dever de notificação? Quando é que esse dever de notificação sobre um determinado incidente de segurança, ele deve acontecer? Como é que a Lei Geral de Proteção de Dados Pessoais, ela estabelece obrigações e a maneira de você traçar todo um plano de comunicação e uma política de gerenciamento de incidentes de segurança? A gente também vai falar isso um pouquinho mais a fundo nessa segunda parte.

Bom, então, colocando o carro, né, na avenida, vamos começar, então, falando um pouquinho mais sobre a Lei Geral de Proteção de Dados Pessoais e procurando enxergar ela como uma janela de oportunidades, não é? Ou seja, como é que ela pode ajudar os próprios times de incidentes de segurança, desde questões, até mesmo em angariar um maior *budget*, um orçamento para a sua respectiva área, até mesmo de você poder, de certa maneira, costurar a narrativa de segurança de redes também muito atrelada, muito junta do discurso da proteção de dados pessoais.

E aqui eu gostaria de já iniciar a nossa conversa quebrando um mito, não é? Que infelizmente ele ainda está muito encrustado nas conversas que a gente vem tendo e como que a gente vê, inclusive, os próprios programas de governança, projetos de adequação se estruturando. É quebrar a ideia de que essa Lei Geral de Proteção de Dados Pessoais, ela vem só para, digamos assim, criar mais um obstáculo para negócios, para a criação de novos modelos de negócios, novas políticas públicas, para a inovação, não é? E não, é justamente o contrário. Essa Lei Geral de Proteção de Dados Pessoais, e isso não é privilégio no Brasil, isso é ao redor do mundo, quando a gente vai olhar para qual é o objetivo, o ponto principal de uma Lei Geral de

Proteção de Dados Pessoais é fazer essa conciliação entre, de um lado, os direitos dos titulares, né, dos dados, nós cidadãos. Nós que utilizamos serviços públicos, nós que utilizamos serviços financeiros, nós que utilizamos uma série de plataformas, e onde os nossos dados, eles trafegam E, ao mesmo tempo, garantir que esses agentes econômicos, eles possam ter uma visão clara do que eles podem ou não fazer, ou pelo menos ter um horizonte onde eles possam se apoiar a esse respeito.

Então uma Lei Geral de Proteção de Dados Pessoais, ela tem essa dupla função, ela não só ajuda e ela não só vislumbra o que deve ser feito para proteger as informações das pessoas, mas ela também procura trazer quase como se fosse um manual de instruções sobre como que agentes econômicos, entidades privadas e entidades públicas, elas podem tratar dados pessoais. E uma das primeiras coisas que qualquer jornada de adequação, ela vai exigir de todos nós, é você organizar a casa. Você arrumar, é aquilo que eu costumo brincar, é quase como se fosse um guarda-roupa de dados. Não tem como você saber quais dados você tem dentro da sua organização antes de você mapeá-los, antes de mapear todos esses processos. Então, uma lei geral de proteção de dados pessoais e, consequentemente, uma jornada de adequação a essa lei, ela cria essa janela de oportunidade para que todas essas organizações, elas possam minimamente criar ordem na informação que elas têm dentro de casa.

E quando você cria ordem nessas informações que você tem dentro de casa, você consegue enxergar melhor qual é esse ativo que você tem e como é que você pode extrair valor desse ativo. Para o campo de segurança de redes, para essa comunidade, a gente sabe muito bem que não tem como você criar uma infraestrutura segura se você não conhece qual é essa infraestrutura que você tem. Não tem como você criar padrões de segurança se você não sabe quais são os bancos de dados que você tem dentro da organização. Quem acessa, como acessa e assim por diante.

Então, ao longo... desde que a Lei Geral de Proteção de Dados Pessoais, ela foi aprovada, tem uma comunidade que está conseguindo fazer desse limão uma limonada, que é justamente o pessoal de segurança de redes. Porque esse é um pilar essencial para um projeto de adequação à Lei Geral de Proteção de Dados Pessoais. Ou seja, você garantir a integridade, a disponibilidade, a acessibilidade desses bancos de dados, e tudo isso em um ambiente seguro.

Então, o que a gente tem visto? E aí é por que a Lei Geral de Proteção de Dados Pessoais ela é uma amiga, e não uma inimiga, é que ela é uma janela de oportunidade para que esses times que durante muito tempo já vem batalhando por criar os seus próprios

budgets, as suas próprias áreas, ou mesmo ampliar o seu orçamento, estão conseguindo ter agora, nessa jornada de adequação.

E isso é um investimento que vale a pena, não é? Agora, onde a gente está em um cenário em que as organizações, elas já estão, se não concluindo os seus projetos de adequação, mas algumas muito próximo disso, a gente já está vendo alguns relatórios nos quais se aponta que: as organizações, elas estão recuperando esse investimento e, inclusive, digamos assim, já colhendo os frutos disso tudo. Ou seja, o valor que você investe em um projeto de adequação, ou mesmo, aqui no caso, em um importante pilar que é esse de segurança dessas informações, ele compensa. Ele *pays off* nesse sentido. E aí 40% dessas organizações já estão percebendo o benefício que você consegue alcançar na estruturação de todos esses processos.

Então, a primeira coisa que eu gostaria aqui, já, de iniciar essa conversa com vocês, é de realmente pensar que essa Lei Geral de Proteção de Dados Pessoais, e essa jornada de adequação, ela é uma janela de oportunidade. Você tem aí uma mentalidade que olha não apenas como mais uma lei que deve ser cumprida no Brasil, que, digamos assim, aumentaria o custo-Brasil, mas como uma lei que ela pode ser, digamos assim, uma atração, algo que catapulta a organização dos processos em várias entidades.

E aí você começa a olhar para tudo isso não apenas para manter e para rever os produtos já existentes, mas para criar novos produtos e rever modelos de negócio, ou mesmo de políticas públicas. E que desde a criação, da concepção disso tudo, a própria perspectiva de segurança já esteja ali desde o início, não é? A gente sabe que, muitas vezes, alguns produtos, eles são lançados e o time de segurança, muitas vezes, é envolvido só na parte final. Essa é o pior cenário onde a gente poderia esperar disso. Então, esses projetos de adequação também já estão servindo para que os times, eles estejam mais sincronizados na medida do possível. Então, você sai de uma análise onde essa lei, ela só vale para você diagnosticar riscos, mas que você consegue também trabalhar com a análise de que existe um valor agregado que pode ser ali gerado. Uma inovação, com base nesses dados e que, esses dados, eles vão ser, sobretudo, tratados em ambiente seguro.

E aí você começa a trabalhar com a ideia de que essa reputação não vai ser calibrada apenas com eventuais sanções que podem sobrevir, por exemplo, se há um vazamento de dados. Mas você pode trabalhar com a reputação que é calibrada muito mais na transparência e na prevenção desses possíveis incidentes de segurança.

Então, para a gente poder aqui já alinhar o discurso, me parece que é muito mais vantajoso, de qualquer área que vai trabalhar nesse projeto, e aí especificamente as áreas dos departamentos de

segurança da informação, segurança de redes, olhar para a Lei Geral de Proteção de Dados Pessoais não como um obstáculo, não como uma lombada ali na frente da sua estrada, que você tem que percorrer, e que isso geraria mais... menos inovação, menos inovação, menos competitividade e menos reputação. Não, pode trabalhar com a ideia de trazer mais inovação, mais competitividade e mais reputação.

Bruno, agora, do ponto de vista prático. Eu entendi o discurso, eu entendo a narrativa, eu entendi onde eu me insiro quando eu vou entrar em uma reunião onde tem aquele departamento jurídico, aquele departamento de *compliance*, mas eu quero entender do ponto de vista mais material, mais concreto, o que isso me ajuda quando eu estou com i meu time, por exemplo, tratando dados, que podem ser pessoais ou não, para combates a incidentes de segurança na rede como um todo.

A Lei Geral de Proteção de Dados Pessoais, e por isso que ela trabalha muito com aquela lógica de uma dupla função. Ela não ajuda apenas o titular, mas ajuda também as organizações que tratam esses dados e o faz de maneira responsável. Ela vai dizer o seguinte: Olha, se você conseguir cumprir com as regras do jogo, surge para você um direito de tratar esses dados. Ou seja, não é apenas o titular que tem direito, mas as organizações que também faz um uso responsável desses dados. E esse voto de confiança, ele é externado quando a gente vai olhar para o fato de que essa Lei Geral de Proteção de Dados Pessoais, ela traz dez hipóteses, dez opções nas quais as organizações, elas podem se apoiar para dar lastro para as suas atividades de tratamento de dados pessoais.

Qual é a grande mudança de cenário? Você não tem que recorrer sempre ao consentimento do titular dos dados, à autorização do cidadão para tratar os seus respectivos dados pessoais. Não, consentimento é apenas uma das dez bases legais ali em cena. A nossa lei, inclusive, a brasileira, ela é, talvez, a mais flexível em comparação a outras leis no direito comparado, ou outras leis estrangeiras. Porque ela tem esse cardápio realmente mais robusto, mais popular.

Então, isso traz necessariamente maior flexibilidade para que as organizações, elas possam tratar dados pessoais. E isso impacta positivamente um grupo específico dessa organização, que é onde a gente está fazendo essa conversa, o departamento ou as pessoas que estão encarregadas de olhar para a segurança da informação, para olhar para a segurança dos dados dentro de uma organização.

A gente sabe que muitas vezes para você garantir um ambiente seguro, você necessita, por exemplo, de fazer o monitoramento do ambiente de trabalho. Monitorar quem acessa, quando acessa, como acessa, se esse acesso vem de um ambiente externo ou interno. Inclusive, monitorar se há uma segmentação física e não apenas lógica

das bases de dados de quem vai acessar aquela sala onde está aquele determinado servidor, ou assim por diante. Então, o monitoramento do ambiente de trabalho que olha para um dos gargalos de segurança da informação, que é o elemento humano, ele envolve, e sempre envolverá, o tratamento de dados pessoais, de como o seu colaborador, ele pode ou não pode acessar determinadas base de dados. E quando ele acessa ou ele carrega consigo uma determinada vulnerabilidade, como é que a coleta desses dados do acesso à sua base de dados, aquilo gera um registro, gera um histórico, um log para tudo isso.

Invariavelmente, de novo, isso vai poder cair na definição de dado pessoal. E aí a primeira pergunta que se faz é: Bruno, eu vou precisar ter o consentimento do colaborador para poder tratar esses dados pessoais? Não. A Lei Geral de Proteção de Dados Pessoais, de novo, ela trouxe dez bases legais que vão muito além do consentimento. E uma das novidades efetivas que surgiram com a Lei Geral de Proteção de Dados Pessoais é o famoso legítimo interesse. Existe um legítimo interesse dessas organizações, públicas e privadas, de que elas garantam segurança a uma infraestrutura onde você pode garantir a integridade dessas informações e o uso não acidental ou externo por terceiros. Consequentemente, você vai poder, enquanto organização, criar e tratar esses dados se valendo dessa base legal, em específico, a do legítimo interesse. Porque existe um legítimo interesse dessas organizações em criar e efetivamente manipular esses dados.

Aqui, então, eu estou trabalhando ainda do ponto de vista de uma perspectiva mais de prevenção. Como esse monitoramento antecipa eventuais incidentes de segurança. Mas, Bruno, a gente sabe que muitas vezes o problema não é se eu vou enfrentar um incidente de segurança, mas quando. A gente está vendo várias organizações que têm bastante maturidade sofrendo determinados ataques e sofrendo determinadas exposições. E depois que isso acontece? Depois que isso aconteceu tenho que gerenciar esse incidente de segurança. Eu tenho que, inclusive, fazer uma investigação interna. De onde veio aquela vulnerabilidade, quem eventualmente vazou aquele determinado dado, se foi um colaborador meu. Como isso aconteceu. De novo, eu vou me encontrar no cenário onde eu vou, enquanto organização, precisar tratar dados pessoais.

E aí, mais uma vez, a Lei Geral de Proteção de Dados Pessoais, ela é amiga, porque você vai poder fazer essas investigações internas, sem necessariamente ter que pedir o consentimento ou a autorização daquelas possíveis pessoas que estão, inclusive, eventualmente suspeitas dentro desse processo de vulnerabilidade, desse incidente de segurança experimentado, porque existe uma base legal, de novo, legítimo interesse, para poder lhe amparar a respeito disso.

E, por fim, a gente sabe que aquelas organizações que têm um maior nível de maturidade, inclusive têm centros de respostas de incidentes de segurança. E esses centros de respostas de incidentes de segurança, eles criam, inclusive, uma rede onde eles trocam informações sobre os ataques que eles estão recebendo, trocam informações como, por exemplo, da onde está partindo aquele ataque, como, por exemplo, um endereço IP, e o endereço IP pode ser considerado dado pessoal, entre outras informações que também poderiam cair nesse conceito de dados pessoal.

Mais uma vez, a Lei Geral de Proteção de Dados Pessoais, ela vai trazer segurança jurídica para que esses centros de respostas de incidentes de segurança continuem a fazer o que eles já fazem há muito tempo, sobretudo, trocando essas informações, entre si, para criar redes de inteligência sobre respostas de incidentes de segurança e coordenar essas respostas. Mais uma vez, você não vai precisar olhar para o consentimento do titular do dado. Até porque isso seria impossível de ser alcançado, e talvez nem mesmo o desejável, mas, de novo, entra aí essa base que eu mencionei do legítimo interesse.

Inclusive, só para vocês terem uma dimensão de como leis de proteção de dados pessoais são, de fato, amigas, né, desse campo, dessa comunidade, que a gente está aqui, hoje, palestrando, para essa audiência, inclusive, a GDPR, ou seja, o regulamento europeu de proteção de dados pessoais traz nas suas considerandas, que é quase como se fosse uma exposição de motivos do porquê a lei veio, que Certs e Csirts podem tratar dados pessoais se valendo do legítimo interesse porque seria dessa maneira pela qual você conseguiria escalar essa operações como um todo. Ou seja, a lei europeia, que a nossa lei brasileira, inclusive, se inspirou muito, chegou a dar nome aos bois. Chegou, inclusive, a falar: olha, centros de respostas de incidentes de segurança, vocês podem se apoiar nessa Lei Geral de Proteção de Dados Pessoais para isso criar segurança para o que vocês já o fazem há muito tempo.

Então, dentro dessa perspectiva, me parece que é claro que a Lei Geral de Proteção de Dados Pessoais, ela abre uma janela de oportunidade, desde para angariar recursos, desde para criar determinados departamentos, até você ter segurança jurídica de que, havendo tratamento desses dados pessoais para viabilizar um ambiente seguro, você o pode fazer e você encontra lastro, bases legais para você operacionalizar.

Bom, o segundo ponto que eu gostaria de trabalhar com vocês é que, de fato, a Lei Geral de Proteção de Dados, ela entende e encara segurança da informação como um dos pilares de proteção de dados pessoais. E ela vai, inclusive, ter um capítulo como um todo, onde ele fala de boas práticas, onde ele vai ser, inclusive, muito minucioso,

muito detalhado de como você tem que, enquanto organização, criar toda essa infraestrutura de segurança.

Pela primeira vez, talvez, a gente tenha, no Brasil, uma lei que chegou a fazer esse tipo de salto, esse tipo de diálogo com esse campo de segurança da informação. Então eu estou falando realmente de lei, pessoal, não de portaria do Bacen, portaria ou outras normas infralegais, decretos do Poder Executivo e assim por diante.

A Lei Geral de Dados Pessoais ela vai criar todo esse capítulo que eu mencionei, onde ela vai dizer o seguinte: Olha, primeiro, antes de mais nada, as organizações elas precisam pensar em quais são as medidas para que você crie uma infraestrutura segura. Essa medida envolve não apenas questões de segurança em sentido lato, mas isso desdobra em medidas técnicas, então, como que a própria e tecnologia pode auxiliar isso, então desde duplo fator de autenticação, como criptografia, até questões mesmo administrativas, ou seja, não basta apenas você ter uma boa tecnologia por trás rodando, mas você também saber que quando um determinado, por exemplo, colaborador era desligado, consequentemente o seu acesso deve ser cancelado. Isso é uma medida administrativa, que tem que haver uma sincronização entre departamento de recursos humanos e departamento de segurança da informação.

Isso tudo deve ser adotado desde o momento da concepção de um produto ou serviço, que é de [ininteligível] *by design*, ou *data security by design*. Essa é uma ideia muito potente, porque como vocês sabem melhor do que eu, por vezes o departamento de segurança era um dos últimos envolvidos quando você tinha um novo produto ou um novo serviço. Isso tem que mudar, tem que haver uma mudança de cultura organizacional.

E a gente vai ter um novo entrante, digamos assim, nesse ecossistema, que é a Autoridade Nacional de Proteção de Dados Pessoais. Então, sim, se espera que essa autoridade possa ser um canal e, sobretudo, uma maneira pela qual a gente possa se apoiar e estabelecer diálogo.

A Autoridade Nacional de Proteção de Dados Pessoais acabou de ser instalada, se espera que ela possa contar com o apoio, inclusive, dessa comunidade de experts para que se quando ela for traçar algum regulamento relacionado a segurança de informação, segurança de redes, ela possa fazer isso da maneira melhor possível, mais bem informada.

E aqui vai um convite. Ano que vem é um ano estratégico para a definição dessas regras do jogo. A autoridade, ela tem que chamar consultas públicas. Isso é um dever dela. Está na Lei Geral de Proteção de Dados Pessoais. Então se espera que essa comunidade também

possa engajar. É um convite aqui, que eu faço, enquanto pesquisador desse tema.

Tudo isso se desdobrar em medidas para que essa proteção evite acessos não autorizados, destruição, perda, alteração. Eu não vou rezar aqui a missa para o vigário. Vocês sabem melhor do que eu.

E um ponto importantíssimo, que é a definição de papéis e responsabilidades. A gente está vivendo um cenário, e o Ministério da Saúde que não nos deixa mentir, daqui a pouco eu falar um pouquinho especificamente desse caso, onde que muitas vezes o ponto de vulnerabilidade não é da própria organização, mas dos parceiros que entram, digamos assim, nessa cadeia.

Então a Lei Geral de Proteção de Dados Pessoais vai trazer essa definição, esse conceito de agentes de tratamento de dados pessoais que se subdividem em dois: controlador e operador.

Em termos claros, controlador é quem controla, quem manda, quem decide; operador é quem trata dados pessoais seguindo as instruções do controlador.

Então, necessariamente quando a gente olhar para esse desenho onde vai haver a cooperação, ou até mesmo uma terceirização de parte de tratamento de dados pessoais, um dos pontos principais é definir quem é quem nessa cadeia. E havendo um parceiro nisso tudo, quais são as obrigações que ele detêm a respeito disso. Ele deve, por exemplo, me notificar se ele é exposto ou se ele sofre um determinado ataque? Se é um incidente de segurança do lado dele que pode me afetar, porque tem ali uma parcela das bases do banco de dados que eu repassei para ele. Ele deve se obrigar a garantir todas essas medidas de segurança da informação que eu tenho que garantir pela Lei Geral de Proteção de Dados Pessoais? Se ele não garante, quais são as implicações contratuais de tudo isso?

É isso que está, por exemplo, sendo discutido agora, nesse caso que eu mencionei do Ministério da Saúde. Qual é a parcela de responsabilidade do Hospital Albert Einstein se, de fato, o incidente de segurança aconteceu em razão de um colaborador que estava ali alocado, e sob as instruções desse hospital em específico e não do Ministério da Saúde. Ambos podem ser responsabilizados? Sim, a nossa Lei Geral de Proteção de Dados Pessoais fala que essa responsabilidade é solidária.

Bom, Bruno, entendi que, de fato, essa Lei Geral de Proteção de Dados Pessoais estabelece um convite, uma ponte para diálogo. Inclusive trabalha no vocabulário que por nós já era trabalhada há muito tempo do campo de segurança das redes.

Agora, efetivamente você já falou que ela pode ser nossa amiga. Agora, quais são as novas fronteiras que essa Lei Geral de Proteção de

Dados Pessoais estabelece para a nossa comunidade, para a nossa atuação.

E aqui eu gosto sempre de trazer esse site, não sei se vocês já tiveram acesso, mas é um site que ele computa, ele contabiliza, os principais incidentes de segurança ao redor do mundo, os principais *leaks*, né? Aí você consegue ter tanto uma dimensão por setor, quanto uma dimensão por gravidade, se você considerar o volume de dados comprometidos e a quantidade de titulares, de pessoas ali expostas.

Essa imagem, ela deixa claro, mais uma vez, que qualquer organização está sujeita a isso. De novo, talvez o mantra que a gente tenha que repetir não é se a minha organização um dia vai ter um incidente de segurança, mas quando ela tiver, como que eu gerencio isso da melhor forma possível. Uma abordagem bastante pragmática e bastante realista.

E aqui, eu acho que vale a pena a gente pegar o caso do Ministério da Saúde para fazer alguns apontamentos e te mesmo algumas generalizações.

Talvez esse seja o principal incidente de segurança da história do Brasil, 16 milhões de brasileiros tiveram os seus dados expostos, dados, inclusive, sensíveis, relacionados ao estado de saúde deles e delas.

E aí, Bruno, dentro desse cenário, o que a Lei Geral de Proteção de Dados Pessoais traz de novo e que não era, até então, experimentado, ou que não era até então considerado quando incidente de segurança acontecia?

O primeiro ponto que eu acho que é importante de reconstruir nessa linha desse incidente de insegurança, é que de acordo com o que parece, algumas vulnerabilidade já haviam sido, inclusive, informadas ao Ministério da Saúde. Na sexta-feira ou na quinta-feira a Open Knowledge Foundation inclusive publicou no seu site uma ata notarial onde ela já tinha avisado, já tinha externado preocupações de como que a própria interface tinha determinadas vulnerabilidade, para além do episódio em si, que foi aberto, todas as credenciais no Github, nessa plataforma onde programadores trocam informações e esses, digamos assim, códigos fontes. Um erro assim, muito, digamos assim, de principiante mesmo. Vocês podem fazer um juízo melhor do que eu, de valor, nesses temas.

Bom, dentro desse cenário, Bruno, a primeira pergunta que se faz, se houve ou não já uma indicação de uma determinada vulnerabilidade, e depois disso ter se tornado público, a primeira questão que se coloca é: Já existia ou existe, pelo menos agora, uma obrigação de notificação de incidente de segurança no Brasil? Essa é uma pergunta crucial. Primeiro porque havia muita controvérsia se, de

fato, toda vez que uma organização tivesse um incidente de segurança, ela deveria notificar órgãos reguladores ou até mesmo os titulares de dados como, por exemplo, consumidores.

Quando a gente olha para o Código de Defesa do Consumidor, já havia, digamos assim, um flerte de que isso deveria acontecer, que deveria ser a mesma lógica do recall. Se um carro é comercializado e se descobre um determinado defeito dele, que pode comprometer a segurança dessas pessoas, por que não aplicar isso para o ponto de vista de um comprometimento da segurança informacional de um produto ou serviço? Mas, de novo, isso era ainda muito debatido, havia muita disputa.

A Lei do Cadastro Positivo, que impacta em cheio as instituições financeiras. Ela falava de procedimentos na hipótese em que houvesse o vazamento de informações ou incidentes de segurança. E aí ela já falava, pelo menos para esse setor específico, que essa comunicação deveria ou poderia se dar para órgãos reguladores como Bacen, Senacon e, em algumas situações, até mesmo os consumidores.

A nova política de segurança cibernética, de 2018, do Banco Central, deixou isso às claras, pelo menos para esse setor, falando, inclusive, de procedimentos para respostas a incidente de segurança. Então criou, de fato, essa obrigatoriedade. Mas, de novo, para um setor muito específico de todo o ecossistema que a gente se depara, hoje, no Brasil.

E pelo menos para organizações listadas no mercado de valores imobiliários, ou seja, que tem ações, isso já era entendido como fato relevante, onde isso poderia afetar a própria confiança dos acionistas daquela organização. Então já havia, pelo nesse mercado como um todo, essa interpretação de que essa obrigatoriedade já existia ou ela seria bastante recomendada.

Bruno, por que tudo isso? Que a gente sabe que hoje o grau de confiança de uma determinada organização passa, necessariamente, pelo grau de maturidade de que ela tem relacionado a segurança. Isso fica claro quando a gente cruza como que o *valuation* dessa organização, ou como que o preço de mercado dela cai, despenca, quando há um incidente de segurança relacionado a essa organização.

Aqui eu trouxe alguns exemplos, um dos maiores incidentes de segurança envolvendo a Equifax, simplesmente o preço de ação despencou, caiu de 140 para quase 90, 80. Netshoes também, aqui no Brasil, daqui a pouco eu vou falar um pouquinho especificamente desse caso. E Facebook, quando teve Cambridge Analytica, né?

Então, a reputação de uma organização, e o mercado já tem entendido isso cada vez de maneira intensa, é calibrada diretamente

pela maturidade que essa organização tem em termos de segurança da informação

Esse é um outro caso mais próximo de nós. Como que o Banco Inter, as ações caíram, despencaram imediatamente logo após a publicização desse incidente de segurança que ele sofreu ali no ano de 2019, salvo engano.

Então, hoje, qual que é a principal mudança que a Lei Geral de Proteção de Dados Pessoais coloca para nós? Ela vai trazer a obrigatoriedade, ou pelo menos parte disso, de a haver a notificação de um incidente de segurança, para todos os setores. Se antes havia uma discussão se isso era voltado mais para as instituições financeiras, que passou a ver com a política de segurança do Bacen, ou se era somente obrigatório para empresas listadas em bolsas de valores a partir da resolução da CVM, com a Lei Geral de Proteção de Dados Pessoais se passa a régua, e qualquer organização, pouco importa o porte, o tamanho, se é ou não listada na bolsa de valores, se é uma instituição financeira ou não, se há um incidente de segurança, tem que se analisar se esse incidente de segurança acarreta um risco ou um dano relevante. E se a resposta é sim, ela é afirmativa, há obrigatoriedade de tornar isso público ou de notificar.

Então, a gente tende a ver um cenário agora, com a Lei Geral de Proteção de Dados Pessoais, onde, de fato, a gente não vai estar olhando mais só para a ponta do iceberg. Ou seja, aquele cenário de incidente de segurança que acabavam se tornando públicos, ou porque quem violou aquele sistema via vantagem em fazer isso, ou porque a mídia tinha o acesso, mas agora porque, de fato, há essa obrigação legal no Brasil.

Bruno, para quem eu devo notificar isso? Primeiro, se o incidente de segurança acontece por parte do operador, aquele que é, digamos assim, o terceiro, é o terceirizado, ele deve, primeiramente, contatar o controlador, que é quem manda, de fato, na atividade de tratamento de dados pessoais. Depois que ele faz isso, surge a obrigação de você contatar os órgãos reguladores. E aqui, no caso, é a própria Autoridade Nacional de Proteção de Dados Pessoais.

E aí é onde que talvez seja o ponto mais emblemático de tudo isso, a gente também começa a ver um cenário onde os próprios consumidores, os próprios titulares de dados, eles também devem ser notificados. E aí, depois que você notifica um titular, isso tende a se tornar público e, consequentemente, a sua reputação enquanto organização comprometida pode ser bastante negativo esse saldo.

Agora, essa comunicação, ela não adianta você só comunicar dizendo que: Olha, eu tive um incidente de segurança, você tem que comunicar e informar quais são as medidas para reverter esse

processo, como que você está atuando para, de certa maneira, remediar esse incidente de segurança.

Então a Lei Geral de Proteção de Dados Pessoais, nesse sentido, de novo, ela vai ser uma amiga, ela vai ser um manual de instruções de como eu tenho ali uma base mínima de poder fazer esse gerenciamento, descrevendo quais são os dados, quais são os titulares ou o conjunto de volume de pessoas atingidas, as medidas técnicas adotadas para reverter es prejuízo.

E aí vai haver, inclusive, prazos. Aqui de novo tem impacto bastante robusto da Lei Geral de Proteção de Dados Pessoais. Essa comunicação, ela tem que ser, via de regra, imediata. Se você não faz de maneira imediata, dentro de um prazo razoável, e explicitar porque isso não foi feito, ou, e aí é o que se espera da Autoridade Nacional de Proteção de Dados Pessoais, que ela possa traçar um prazo, digamos assim, mais duro para que as próprias organizações, elas possa, de certa maneira, saber até quanto tempo... O que seria esse prazo razoável? Que é muito genético, muito amplo, muito aberto. E aí, a autoridade, ela poderia nos ajudar nesse sentido.

E aí, vale a pena notificar? Por que vale a pena notificar, Bruno? Como que eu devo fazer isso? Que é a segunda parte, e aí eu encaminho para a conclusão.

Eu vou trazer dois casos que já foram objetos de análise por parte do Ministério Público do Distrito Federal, ele celebrou um termo de ajustamento de conduta com essas duas organizações.

E, como vocês podem ver aí na tela, uma organização acabou sendo sancionada em R$ 500 mil, a outra organização em três vezes o valor. Por que isso aconteceu? Porque em um determinado cenário, é isso que dá para extrair dos documentos que se tornaram públicos, aquela primeira organização, ela, de fato, não jogou, digamos assim, incidente de segurança para debaixo do tapete. Tão logo isso aconteceu, ela tornou isso público, houve ali toda uma abordagem de também notificar os próprios titulares de dados. Ela conseguiu operacionalizar isso tudo. Ela conversou com o órgão regulador e explicitou quais eram as medidas adotadas desde o dia em que se tomou conhecimento dessa vulnerabilidade. E aí, o Ministério Público do Distrito Federal falou: Olha, de fato, ainda que a Lei Geral de Proteção de Dados Pessoais não seja aplicável agora, você seguiu toda a receita de bolo, ou pelo menos a base, o mínimo que você deveria ter feito para gerenciar esse incidente de segurança. Você está de boa-fé. E porque você está de boa-fé, eu vou reduzir esse sancionamento, esse porrete mesmo que o órgão regulador poderia dar em cima de você.

O que a gente percebe desde que projetos de adequação começaram a rodar e políticas de gerenciamento de incidentes de

segurança se tornaram cada vez mais maduras? A gente percebe que é um movimento que deve ser holístico dentro de toda organização, inclusive deve envolver vários departamentos para que essa resposta, ela seja a mais uniforme e a mais madura possível. Não basta apenas isso envolver o time de segurança da informação? Sim, na fase de planejamento ele deve fornecer orientações sobre detecção, os recursos humanos e tecnológicos para preservação da integrado desses sistemas. E depois que acontece o incidente, ele deve falar quais são os dados comprometidos e conduzir aquelas investigações que eu mencionei anteriormente, que tem, inclusive, uma base legal destacada para isso. Mas é necessário, por exemplo, envolver o departamento jurídico para entender. Se esse incidente de segurança, por exemplo, se deu no meu parceiro comercial terceirizado, qual que é a responsabilidade dele? E se a responsabilidade dele está clara no instrumento contratual, como que isso eventualmente limita a minha responsabilidade ou com o que isso reduz as minhas consequências econômicas? E como que vou, de fato, quando comunicar isso para fora, fazer isso reduzindo os riscos jurídicos regulatórios?

Eu tenho que contatar diretamente o próprio departamento de recursos humanos para que ele possa, na fase preventiva, treinar essas pessoas, e aí está um grande gargalo. Talvez aí o elemento humano seja o maior ponto de vulnerabilidade, se não há o treinamento dessas pessoas, dificilmente você consegue trazer alguma coisa que seja resiliente e que sirva de canal de comunicação com os próprios empregados quando esse incidente de segurança já aconteceu.

Financeiro, o departamento financeiro, para eventualmente até mesmo fazer projeções de qual é o impacto financeiro disso. Em organizações listadas em bolsa de valores isso fica claro, como trouxe aqueles gráficos.

Assegurar recursos financeiros para a resolução desses incidentes. Então, se eventualmente, por exemplo, não tenho um time capaz de fazer todo o desenho de relações públicas disso, vale a pena contratar uma organização terceira para fazer essa gestão de crise? Qual que é o *budget* para isso? Eu vou acionar o meu seguro cibernético? Qual é o valor que eu tenho que pagar para ser eventualmente coberto? Tem alguma exceção na minha apólice? Qual é essa exceção, ela cobre tudo isso? Tudo isso envolve aí, pelo menos um franco diálogo entre o jurídico e o financeiro.

Marketing, para conceder como que vai se dar esse bom relacionamento com os clientes, estabelecer uma mensagem consistente, positiva com os clientes. Algumas organizações que trouxeram práticas transparentes inclusive conseguiram se consolidar em alguns determinados mercados, extraindo de uma situação negativa algo extremamente positivo. Então vale também a pena

pensar nisso. E até mesmo, aí em último caso, como que esse discurso deve ser alinhado não apenas debaixo para cima, mas de cima para baixo, com o CEO, presidência, e isso, de fato, ser verticalizado por toda a organização.

Então, Bruno, qual que é a sua conclusão? E aqui eu peço só mais um minuto do tempo para chegar no final da minha apresentação. A Lei Geral de Proteção de Dados Pessoais traz, de fato, um novo cenário, eu acho, que para o gerenciamento de incidente de segurança. E vale a pena pensar nisso do ponto de vista de organizar todos esses processos. Porque quanto mais responsável, quanto mais contas forem prestadas a esse respeito, essa ideia de *accountability*, de prestação de contas, mais argumentos você vai ter na mesa para garantir um impacto mais reduzido em termos de imputação, e até mesmo de comprometimento frente ao órgão regulador. Porque isso vai ser levado em consideração. Quanto mais colaborativo, quanto mais responsável for aquela determinada organização, e ela comprovar que ela estabeleceu políticas, investiu em recursos humanos e tecnológicos, fez a gestão de maneira adequada daquele incidente, dando transparência, comunicando o órgão regulador, eventualmente até os titulares notificando-os, isso vai ser computado para eventual sanção. Talvez não uma multa expressiva, mas talvez uma multa mais baixa, como foi o caso da Netshoes comparando com o Banco Inter, ou até mesmo, em última análise, algo que seja mais leve, como, por exemplo, a publicização, mas não necessariamente uma perda financeira, ou até mesmo uma advertência.

Por que, Bruno, isso vale a pena? Porque não é uma faculdade da Autoridade Nacional de Proteção de Dados Pessoais e de outros órgãos reguladores, mas um dever. O art. 52 da nossa Lei Geral de Proteção de Dados Pessoais expressamente diz que a seriedade das sanções, a calibração das penalidades, ela deve seguir essa lógica de um comportamento mais ou menos reprovável. Me parece que isso fica claro no cenário que a gente já está vivendo no Brasil de gerenciamento de incidente de segurança.

Então, efetivamente, me parece que a Lei Geral de Proteção de Dados Pessoais muda muito o cenário, porque ela pode ser uma amiga, aquela primeira parte que eu falei, *budget*, recurso financeiro e assim por diante, e ela também pode ajudar em toda procedimentalização de como que isso já tem acontecido no Brasil.

Então era isso. Eu queria, mais uma vez, agradecer muito o convite. Pedir desculpas porque eu acabei passando pouquinho do meu tempo. E agradecendo, mais uma vez, o convite feito pelo NIC.br para estar aqui hoje com vocês.

SR. RUBENS KUHL: Obrigado, Bruno. A gente tem pouco tempo para perguntas. Então, a única pergunta que a gente vai ter tempo de

fazer é do [ininteligível] Cavalcanti, em que ele cita uma iniciativa do sistema de saúde inglês, o NHS, que é como o SUS de lá, chamada [ininteligível], de dar gestão para os titulares dos dados, de como eles vão ser acessados, de administrar a privacidade deles disso. E a pergunta é: Se você vê isso como tendência? Obrigado. Bruno, você está aí?

SR. BRUNO BIONI: Rubens, só pegar essa última parte aí, que eu não peguei, que o meu fone falhou, da tendência.

SR. RUBENS KUHL: Final era se você vê isso como uma tendência ali, na gestão de dados pessoais.

SR. BRUNO BIONI: Eu acho que sim, acho que essas iniciativas que procuram trazer boas práticas, e até mesmo uma certa padronização, pensando que essa padronização é o mínimo dessa régua, dessa base da pirâmide. Me parece que isso não é só útil como desejável.

Então eu acho que, de novo, para além dessa iniciativa, acho que vale a pena olhar para o ano que vem como um ano bastante crítico e importante. Onde a gente possa também construir um canal de diálogo com a própria Autoridade Nacional de Proteção de Dados Pessoais, porque, invariavelmente, ela vai normatizar e regulamentar essas questões. Basta lembrar que três dos cinco diretores da Autoridade Nacional de Proteção de Dados Pessoais são pessoas que têm uma formação bastante ali, do campo militar, então eles, invariavelmente, tem uma mentalidade mais, digamos assim, próxima de segurança, segurança cibernética.

Então acho que seria isso a minha conclusão final.

SR. FREDERICO NEVES: Bruno, muitíssimo obrigado. Em nome do Comitê de Programa eu quero agradecer você pela exposição tão clara e que pode dar um norte muito bom para as instituições e organizações técnicas aqui da internet no país. Muito obrigado, viu?

E agora, para continuar, a gente vai ter o Leandro Bertholdo fazendo uma apresentação para a gente sobre o BGP Anycast Tuner, gerenciamento intuitivo para serviços Anycast. Leandro, por favor.

SR. LEANDRO BERTOLDO: Alô, oi. Deixa eu ver se estou mutado aqui ou não.

SR. FREDERICO NEVES: Estamos te ouvindo sim.

SR. LEANDRO BERTHOLDO: Ok, perfeito.

Bom, primeiro de tudo, tenho que só agradecer a Profa. Ariane pela lembrança. E, graças a ela, eu consegui ter vários desafios na vida bem interessantes. Então, antes de mais nada, antes de começar, o meu agradecimento a ela.

Bom, eu vou falar para vocês aqui de uma ferramenta que a gente desenvolveu chamada de BGP Anycast Tuner para gerenciamento de serviços Anycast.

A ideia aqui é conseguir prover para os operadores de redes Anycast uma melhor gerência visando, exatamente, ajudar nessa parte de mitigação de ataques DDoS.

Bom, primeiro, o que é uma rede Anycast e o que é o conceito de catchment que a gente chama? Uma rede Anycast basicamente é o mesmo prefixo de rede que é divulgado em vários locais diferentes da internet, exatamente o mesmo prefixo, e a ideia aqui é deixar o protocolo BGP decidir qual cliente que vai ser atendido por qual servidor.

Então basicamente aqui, a gente tem, por exemplo, o site azul que tem catchment dos clientes 2 e 3. Então, o nosso desafio aqui é: Como é que a gente faria o melhor balanceamento para o cliente 2, por exemplo, usar este outro caminho dentro do BGP para chegar dentro desse site vermelho. Essa é a ideia inicial do projeto.

E como é que a gente gerencia isso e como é que a gente contabiliza isso? Bom, o gerenciamento do serviço Anycast, ele é complicado, não é tão simples quando aparenta porque envolve todas as métricas do BGP, e é complicado fazer esse mapeamento do ponto de vista de alguém que está conectado na internet. Então essa amarração do BGP, ela complica bastante.

A maioria das CDNs usa o DNS e faz o balanceamento em cima do DNS, ou seja, verifica qual é o cliente e aí, a localização geográfica, o posicionamento geográfico daquele cliente, ou o IP que ele está utilizando, escolhe um site para ele. Então DNS acaba sendo a parte básica antes das outras informações de aplicação para CDN. Então o nosso problema é como é que a gente faz para balancear o próprio servidor de DNS.

Na maioria dos CCQLDs como o NIC.br, o [ininteligível], eles possuem próprias redes Anycast, mas normalmente cada prefixo tem até 20 sites que ele está usando. Claro que redes Anycast e provedores CDN, como o Cloudy Flare, tem mais de mil sites. Então a abordagem dessa ferramenta é para esses CCQLDs ou informações, ou empresas que tem o serviço Anycast até 20, 30 sites.

Bom, nossas questões aqui são as seguintes: Como é que a gente faz para otimizar esse desempenho? Como é que a gente melhora o balanceamento de carga? E como é que a gente, principalmente, prevê o comportamento da rede quando a gente muda a política de BGP de alguns dos sites? Então a nossa ideia aqui é tentar prever o que acontece e qual o impacto de uma mudança no BGP e um daqueles

sites. E a ideia aqui é definir quais são os requisitos que a gente tem para conseguir fazer a gerência desse serviço de Anycast.

Então a gente mapeou uns requisitos iniciais, do tipo que a gente viu que a gente precisava ter algum tipo de mapeamento desses catchments, a gente precisava ter um controle sobre esses catchments, precisamos ter algum tipo de métrica ou suporte, a métrica apurável(F), vamos dizer assim, que eu posso querer escolher por catchment, por país, por RTT, várias métricas em coima do serviço Anycast, e eu preciso ter alguma maneira de fazer isso de forma automatizada, para descobrir quais são as engenharias de trafego que estão ativas em cada um dos nossos clientes ou em cada uma das redes onde a gente está atendendo instituições.

E isso tudo tem que funcionar de uma forma atômica. Ou seja, se eu mexer na configuração de um servidor Anycast, isso tem que funcionar para todos os outros. E, no final, a gente precisa ter uma maneira fácil de gerenciar isso. Então esse era o nosso desafio inicial.

Para isso o que a gente fez? A gente pegou uma abordagem onde a gente, primeiro, coleta todas as políticas de roteamento que a gente tem, de cada um desses sites, se o nosso provedor de trânsito provê por [ininteligível], se ele provê comunidades BGP, se o Internet Exchange que a gente está conectado, que tipo de alcançabilidade, ou que tipo de feature, que tipo de variação nas políticas de BGP a gente pode usar para fazer uma mudança, por exemplo, em um caso de ataque.

Então a ideia aqui é a seguinte, coleta todas essas políticas BGP, faz o deploy de uma política dessas, ou seja, configura ela, faz uma série de medidas para verificar como é que está o catchment dessa política, e aí a gente faz uma separação dos resultados, que são úteis do ponto de vista de engenharia de tráfego ou mudança relativa a deslocamento de tráfego entre sites Anycast, e salvo isso no que a gente chama de um BGP Cookbook. Ou seja, um livro de receitas onde a gente tem o sucesso de uma determina política. As outras políticas a gente, ou ignora ou deixa ela para casos mais específicos. E a gente fica nesse *loop* para detectar todas as políticas possíveis em cada um dos sites.

Como vocês podem imaginar, aqui tem um volume bem grande de possibilidades que podem ser testadas em cada um dos sites. Para isso a gente um algoritmo de otimização também.

Bom, como que é que a gente testou? A gente usou um laboratório que a gente construiu, que é um testbed espalhado aí, em vários sites do mundo, chamado Tangled. E a gente concluiu botar vários [ininteligível] ao longo dos anos nesses sites, principalmente com apoio, ou dos CCTLDs como [ininteligível], na Holanda, ou o da Dinamarca, e várias universidades onde a gente desenvolveu isso.

Basicamente a gente usa um prefixo B4(F) ou prefixo B6(F), e a gente desenvolveu algumas ferramentas para, por exemplo, monitorar quais são as seções que estão estabelecidas, não estão estabelecidas, e manipulação desse prefixo BGP.

Essa interface pode ser uma interface [ininteligível] ou pode ser uma interface web service, onde o administrador pode ativar ou desativar o prefixo em algum determinado site.

Aqui tem mais ou menos a interface como é que ela funciona, onde a gente consegue, por exemplo, nesse primeiro exemplo aqui em cima, verificar ou enviar um determinado prefixo para um site específico na França, anunciando uma parte do nosso bloco lá com alguns [ininteligível]. Então esse é o tipo de funcionalidade que está previsto nessas ferramentas.

Que tipo de experimento que a gente fez? Bom, para fazer coleta dos dados foi desenvolvido na universidade uma ferramenta chamada Verfploeter. A Verfploeter é uma palavra em holandês que quer dizer deixar pegar, como pintar com os pés, algo parecido com isso.

A ideia aqui é a seguinte, baseado em uma rede [ininteligível] que foi desenvolvida pelo pessoal da [ininteligível], da Universidade Sul da Califórnia, a gente realiza peerings em aproximadamente 6 milhões de endereços. Então, uma máquina envia esses peerings para máquinas, que geralmente são hosts responsivos espalhados pelo mundo, e a gente coleta os resultados determinando qual é o inbound de uma determinada rede.

Então, por exemplo, se eu estiver na UFRGS, a UFRGS vai responder para o [ininteligível] que está em Porto Alegre, que é o [ininteligível] mais próximo. Se eu estiver na Holanda, o endereço de um determinado provedor na Holanda vai responder para o site mais próximo que está na Holanda, e assim por diante.

Então, com isso a gente consegue fazer o mapeamento de todo tráfego inbound em cada um de... por volta de 4 milhões de prefixos que a gente tema resposta. Prefixos /24.

Como é que funciona aqui? A gente faz as medições a cada 15 minutos. Então a gente tem por volta de 4 milhões de redes /24, que a gente tem, e a gente consegue estabelecer quais são as políticas individuais de cada uma dessas redes finais. Então, com isso, a gente consegue, por exemplo, faz uma série de medições, estabelece um *base line* dessas medições, mantém essas medições regulares de tempos em tempos, e explora, eventualmente, algumas medições adicionais que a gente precisa. Como, por exemplo, tentar alguma comunidade específica ou algo assim.

E aí a gente consegue ter vários *insights* em como a nossa rede Anycast captura esse catchment. Basicamente o que a gente pega, a

gente tem, por exemplo, catchment e distribuição de carga como uma das métrica que a gente utiliza.

Então aqui, por exemplo, uma linha onde a gente pode fazer um anúncio para determinado site, eventualmente pode usar comunidades de blackhole para aquele site, ou não, dependendo do que provedor nos permite, para bloquear um determinado DDoS, uma determinada região.

Bom, no final, a gente tinha uma base de 300 milhões de respostas para analisar. Isso é algo que nos dá bastante trabalho na forma de ponto de vista de reconhecimento da própria rede Anycast. Então, a cada 15 minutos a gente executa 6 milhões, e a gente muda esse anúncio BGP e faz um novo teste. E aí a gente contabiliza tudo isso. A gente tem dois tipos de medição, uma medição individual ou uma medição regular, de tempos em tempos.

Tem um fato interessante a respeito de catchment, que são de outros trabalhos, que diz que o catchment é algo estável, dificilmente muda ao longo do tempo. E a gente viu que isso realmente é verdade, em períodos de meses. Então, salvo quando algum grande provedor resolve mudar a sua conexão para um Internet Exchange, ou estabelecer ou desestabelecer uma política entre duas grandes redes, esse catchment é razoavelmente estável.

Aqui, por exemplo, quando a gente estava processando o quanto consome de dados e de CPU para resolver esse problema, ou para estabelecer essas políticas, e qual o impacto dela nos catchments. Para isso a gente desenvolveu algumas ferramentas, uma delas é o [ininteligível] para fazer análise dos dados. Então a gente tem uma visão rápida de como é que esses dados se comportam ao longo do tempo, sem fazer uma análise mais detalhada. E a gente tem uma outra ferramenta que é para... que é um dashboard para analisar como é que está essa distribuição entre os vários países. Depois a gente dá uma olhada em uma animaçãozinha ali.

Bom, a gente pode analisar a partir de catchment, a partir de geolocalização de cada um deles e tentar manipular em cima deles, ou em cima de RTT para tentar melhorar a experiência do usuário.

Então aqui, por exemplo, temos um exemplo nos Estados Unidos, e a gente tem qual é o RTT máximo, que seria 99 [ininteligível] que a gente pega para cada um deles, que aí está em torno de 600 milissegundos, e qual é a perda eventual que a gente está reconhecendo em determinados sites. Então a gente usa essas métrica para tentar calcular qual é a melhor configuração do BGP para essa rede.

Bom, o nosso problema é o seguinte, como vocês viram, a gente gera uma quantidade bem grande de dados. Isso é a nossa maneira

de monitorar o serviço Anycast. Mas a nossa proposta aqui é como é que a gente altera essa visibilidade dos sites. Esse é o ponto principal.

Então, para alterar isso, a gente tem que fazer manipulação dos anúncios BGP. Então a gente testou algumas coisas do tipo: Ok, vou testar essa por [ininteligível], vou testar comunidades. E aí a gente queria avaliar o quão granular é esse controle, quanto tempo leva para implementar uma mudança dentro do BGP, para que esses sites Anycast sintam, e qual é a visibilidade dos prefixos após essa mudança.

Então, aqui, por exemplo, um comportamento normal, um determinado cliente está mandando seus dados lá para o SIDN(F) na Holanda. Em Anycast algumas vezes a gente tem uma série de ataques que sobrecarregam aquele site. A ideia aqui é piorar o acesso àquele site para aquele cliente específico de forma que ele escolha algum outro site. E aí a gente consegue balancear essa carga de ataque ou eventualmente direcionar para um site maior.

Então, assim como o cliente vai para um determinado site, os ataques podem ir para esse outro site, que é um pouco maior, que pode manusear esses ataques.

O tempo de convergência para isso que a gente concluiu no BGP, para o pior caso, é em torno de dez minutos, o melhor caso é algo em torno de três minutos.

Bom, com isso a gente cria basicamente uma *base line*, ou seja, qual é o catchment que a gente tem a distribuição em cima da nossa rede para uma determinada rede origem, e aí a gente vai fazer avaliações, como, por exemplo, o caso do prepend. Então a gente pega um prefixo, vê que o prefixo está aqui, e a gente altera essa preferência, por exemplo, artificialmente modificando o as_path, ou piorando o caminho até aquele nosso site, que faz com que o cliente possa ir ou não para determinado... possa ser modificado de um determinado site para outro.

E aí, como existem algumas diferenças na biografia quanto aqui as_path, a prepend funciona ou não funciona, a gente fez os nossos próprios testes usando essa ferramenta de medição Anycast. Então a gente colocou determinados prepends, e a gente notou o seguinte, que no caso específico de prepends, aqui para a direita isso é a nossa *base line*, ou seja, sem ter o BGP modificado. Isso aqui é a visão de um site específico, que é o site da França. E a gente pode ver aqui que quando a gente faz um prepend, que é para o lado direito, eu tenho alguma parte do tráfego que é mudado, algo em torno de 7%.

Só que depois do primeiro prepend eu não tenho mais efeito nenhum. Esse comportamento, a gente alterou ele fazendo o que a gente chama de negativo prepend. Negativo prepend é dar, por exemplo, prepend em todos os outros sites, menos nesse, e tentar

quantificar qual é o impacto disso. Isso a gente notou que, por exemplo, no caso de negativo prepend a gente consegue controlar algo em torno de 50% do tráfego. Isso significa que sim, o prepend funciona, só que pode não funcionar em determinados sites.

E aí a gente começou a fazer uma avaliação para todos. Então a nossa ideia aqui é o seguinte, prepend é uma maneira de eu tirar o tráfego de um determinado lugar, e se eu usar o negativo prepend para aquele site, eu consigo atrair mais tráfego para aquele site.

E isso aqui é a curva que a gente tem como resultante de todos os sites e como o prepend funciona. Então, o que a gente viu? Que nos vários sites que a gente realizou esse teste, a gente viu que o prepend sim, funciona, mas até dois prepends, não mais do que isso. Então acima de dois prepends ele fica em uma situação bastante estável.

O negativo prepend é a mesma coisa, aferindo que, com exceção de uma curva aqui, um [ininteligível] que aceitou três prepends, o resto estava funcionando muito bem com dois. Que é onde consegue a menor(F) diferença. O problema é a granularidade. Quando a gente usa prepend a gente não tem um controle granular com o tráfego da mesma forma que a gente tem com comunidades. Então, o que funciona é entre dois e menos dois prepends, ou dois positivos ou dois negativos.

Aqui está o exemplo do site de Paris, onde a gente tem, em azul, a *base line*, e após dar um prepend em Paris, a gente nota que o tráfego foi para Los Angeles, Miami, Porto Alegre, Sidnei, ele se dividiu e foi um pouquinho para cada site.

A gente ampliou isso, por exemplo, para três sites. Então vocês conseguem ver aqui que aqui já tem outras comunidades, não somente... já tem comunidades não somente prepends, então comunidades como No-Export para um determinado provedor, No-[ininteligível] para determinado IXP, a gente consegue um controle mais granular do site.

O problema é que, conforme a gente vai ampliando o número de sites, a gente tem uma variação total no catchment. Ou seja, toda vez que alguém inserir um site novo na rede Anycast, o mapeamento muda quase que completamente.

Então vocês podem ver aqui o mapeamento para três sites, o mapeamento para cinco sites e o mapeamento para sete sites já é totalmente diferente. Então, [ininteligível] é que para cada novo site adicionado a gente teria que recalcular todos esses valores.

Bom, para facilitar a vida a gente usa aquele cookbook baseado nessa história de que uma vez que a gente tem a nossa rede razoavelmente estável, o número de sites para aquele prefixo, eu consigo estabelecer um livro de receitas de políticas BGP. Esse livro de

receitas funciona mais ou menos assim: A gente tem o *base line*, e a gente tem umas políticas, por exemplo, para cima, se eu quiser jogar mais tráfego para o site em Londres. Ok, uma das coisas que eu posso fazer é dar dois prepends em Los Angeles. Se eu der dois prepends em Los Angeles eu [ininteligível] para 25% de tráfego em Londres. Se eu der dois prepends em Miami eu jogo 30% de tráfego em Los Angeles. E se eu dou dois negativos prepends em Los Angeles, eu atraio 64% do tráfego, que é o máximo que eu consigo com essa configuração envolvendo aqui seis sites.

O contrário, para baixo, eu consigo diminuir a carga em Londres. Então conforme o que a gente vai anunciar em Londres, ou em outros sites, esse conjunto de políticas pode diminuir o volume de tráfego em Londres.

Mas o problema é o seguinte, nenhum administrador vai querer olhar essa tabelinha para saber o que ele tem que fazer em um caso, por exemplo, de um ataque ou no caso de alguma configuração de [ininteligível] da rede Anycast. Então, para isso, a gente pensou em um *equalizer* como uma maneira de facilitar a vida do administrador para ele conseguir controlar esse site... essa carga(F) pegando sites.

O nome da solução, vamos dizer assim, é baseado no equalizador. Mas aí o pessoal do [ininteligível] preferiu o nome Tuner, sendo uma maneira de fazer um *tunning* dessa sede Anycast.

Isso aqui é a interface do nosso BGP Tuner. Então, basicamente, o que a gente tem que aqui é o seguinte, é a carga, o número de redes /24 que está indo para um determinado site, uma maneira de ter metas pré-determinadas, como trazer todo o tráfego para os Estados Unidos, ou *presets* de configuração e o que envolve a política para fazer esse preset funcionar. Então essa é a ideia básica.

E aqui a gente tem uma série de sliders(F) onde a gente consegue usar para jogar o tráfego de um determinado site para o outro. Notem que vocês têm vários traços em cada um desses sliders(F). esses traços são construídos a partir de cada uma das políticas específicas para aquele site e mapeadas para dentro do slider(F).

Então, como vocês podem ver, os degraus não são uniforme para cada um porque determinadas políticas tem efeitos diferentes. Então, aqui, por exemplo, está jogando 70% do tráfego para [ininteligível] do site ou diminuindo até 25%. Então existe esse mapeamento entre as políticas e os sliders(F).

Aqui, por exemplo, a gente pode pegar o site de Paris e puxar o slider(F) para cima e fazer com que o tráfego que vá para Paris e ver o impacto nos outros tráfegos.

Então vocês podem ver aqui quantos por cento ou quantas redes /24 está indo para cada um deles. Ou pode escolher trazer determinado... trazer mais tráfego para os Estados Unidos e ver como é que isso aqui se comporta e qual a política que vai ser aplicada.

Essa política, a gente não está fazendo aplicação automática da política, mas é um passo fácil de automação que pode ser implementado.

Outra coisa que foi desenvolvida é um dashborad para inspeção de tráfego. Então a gente pode chegar aqui, por exemplo, selecionar os Estados Unidos, e aí ver quais os clientes dos Estados Unidos que estão indo... são mapeados nos Estados Unidos que estão indo para Londres, e aí a gente vê os principais ASs que estão mandando tráfego, que são ASs alocados dentro dos Estados Unidos e que estão escolhendo mandar tráfego para Londres.

Então essa é a ideia para fazer um *tunning* e ver como é que a gente pode atrair mais tráfego de um site para outro. Ou seja, aqui a gente está mapeando qual é o resultado da política que a gente tem acionado naquele momento

Pois bem, então a gente tinha séria de requisitos e a gente foi avaliar esses requisitos. Então eu preciso ter o mapeamento do meu catchment, eu consigo fazer isso com [ininteligível], é uma ferramenta adequada para isso. Esse mapeamento também pode ser feito baseado em [ininteligível]. Só que como a gente não tem um tráfego real ou serviço real rodando no teste [ininteligível], então a maneira de a gente fazer esse mapeamento é baseado nessa [ininteligível] list. Isso pode ser adequado sem problemas para fluxos.

A gente tem uma maneira de controlar esse [ininteligível], e aí está a ferramenta de *tunning* para fazer isso. A gente suporta várias métricas, embora a maioria das coisas são em cima de catchment, ou seja, esse controle para se determinado cliente vai para um site ou não. Isso pode ser alterado para, por exemplo, geolocalização ou para RTT, ou para qualquer outro tipo, proximidade, por exemplo, TTL, geralmente baseado em alguma informação que a gente tenha dentro do pacote [ininteligível].

A gente tem uma maneira de fazer a descoberta automática dessa engenharia de tráfego. Para isso a gente desenvolveu esse método. A gente suporta de maneira uma rápida de fazer deploy das políticas. Então tem aqui uma meta que pode selecionar e fazer deploy. E a gente tem uma maneira de fazer uma... A gente tem uma interface de gerência simples para o Administrador para conseguir [ininteligível] ou retrair tráfego de determinado local. Isso pode ser usado, por exemplo, em uma manutenção.

Bom, nossa conclusão, fazer essas medições nas redes Anycast é importante exatamente para conhecer o comportamento dessa nossa rede. Isso é interessante do ponto de vista de qualidade e experiência para o usuário. É interessante do ponto de vista de otimização de tráfego. Tem algumas coisas que são relativas, por exemplo, o controle de bordas e políticas de [ininteligível], etc., que também podem ser utilizadas. A manipulação do catchment, a gente viu que a as_prepend funciona até dois prepends. Então ele tem um impacto que varia determinando da posição do nosso provedor de acesso. E a gente conseguiu fazer, no final, uma interface gráfica interessante para os operadores, que é o BGP Tuner, para ajudar a gerenciar essas redes Anycast.

Tem um artigo publicado sobre isso, então mais informações vocês podem encontrar lá. Essa ferramenta está disponível publicamente também. No *paper* está citado onde vocês podem obter ela.

O trabalho foi desenvolvido com esforço conjunto da Universidade Twente, do SIDN, que é responsável pelo domínio .nl(F), pelo Não, senhor.net Labs, que o Roland, que é o meu orientador, participa, e pela Universidade Federal do Rio Grande do Sul. Então foi um esforço aí de várias instituições.

Perfeito. Alguma pergunta?

SR. FREDERICO NEVES: Então, Leandro, deixa eu aproveitar e fazer uma pergunta aqui. Eu vi que no exemplo você, pelo menos no testbed vocês mostram vários casos que aparentam ter, principalmente servidores com trânsito. Mas tem muita rede Anycast que é bastante heterogênea com relação a ter nós globais e com trânsito, e muitos nós locais, principalmente com presença em Internet Exchange, e você tem ainda, nesses casos, a dificuldade maior ainda de você receber muito tráfego nessas localidades e não ter como devolver no próprio Exchange porque você não recebe o prefixo naquele local, você acaba tendo que tunelar(F) isso ou, de algum jeito, fazer isso chegar no cliente, porque você não tem um prefixo para retorno ali.

Como é que vocês lidam com isso? E como é que lidam com a questão da heterogeneidade dessas redes? Porque tem muita rede que pode ser um [ininteligível] global, que tem hardware dedicado de rede e isso daí está misturado com nós locais que está tudo lá dentro de uma máquina fazendo tudo, roteamento, serviço DNS e etc.

SR. LEANDRO BERTOLDO: Tá. Uma das coisas que são parâmetros que a gente chama do modo, então tu tem coisa do tipo que a carga... quando tu está sofrendo um ataque DDoS, ele pode acontecer de várias formas, um deles é ele estar com [ininteligível] simplesmente com a carga mais alta. Então o parâmetro de carga do

site é um dos itens que pode ser utilizado para tirar a carga daquele tráfego ou não, daquele [ininteligível], daquele site ou não. Então uma coisa é a carga. Outra coisa é sim, a gente já notou que tem uma diferença de comportamento bem interessante, principalmente dos provedores Anycast dentro de Internet Exchange ou de outras redes.

Então, tem um outro trabalho que foi apresentado por um colega, eu participei, que é no Anycast, que é uma maneira de a gente localizar essas redes Anycast em diversos locais da Internet. Então a gente usa uma rede Anycast para localizar outra rede Anycast. E isso tem dado resultados excelentes para a gente saber onde é que estão colocados cada um deles.

E sim, o outro item é que determinados sites que estão colocados, por exemplo, dentro dos IXPs não têm o comportamento esperado pelo provedor daquela rede Anycast. E normalmente essa é uma parte da gerência que os administradores dessa rede Anycast não têm e que essa ferramenta ajuda a resolver. Porque normalmente tu quer saber: Ok, eu estou recebendo pouco tráfego, mas eu não estou recebendo o tráfego do fulano, beltrano e ciclano, por quê? O que está acontecendo? Por que esse cara não entrega tráfego lá? Então, com esse mapeamento a gente consegue saber como é que esse tráfego está sendo entregue, aliás, pelo menos onde esse tráfego está sendo entregue e inspecionar uma possível causa de porquê ele está sendo entregue em outro lugar.

Nessa parte de comunidades a gente fez um trabalho para tentar usar, por exemplo, comunidade seletiva para marcar exatamente quem deve entregar tráfego para um determinado prefixo dentro da Internet Exchange. Isso é um outro trabalho que foi enviado para o [ininteligível] agora a pouco, mas ainda não temos informação se ele foi aceito ou não.

SR. FREDERICO NEVES: Vocês não tentaram nada com uso de [ininteligível]?

SR. LEANDRO BERTOLDO: Não, não. Porque uma das coisas que a gente encontrou é o seguinte, eu tenho médio que eu posso usar para controlar, eu comunidades e eu tenho prepends. Então, o nosso problema é o seguinte, se eu chegar em um Internet Exchange que tem que mil participantes, como o de São Paulo, ou 2 mil, e eu tentar todas as combinações possíveis, eu vou para um problema exponencial. E, do ponto de vista de análise que a gente fez, é possível fazer isso sim. Mas o que a gente analisou é o seguinte, se eu fizer isso, a gente fez esse teste em São Paulo, eu tenho os primeiros cem ASs que me dão algum retorno razoável, os outros, a carga é tão baixa que é desprezível, do ponto de vista de uma rede Anycast global.

Então a gente fez esse exercício, mas aí viu que não valia a pena seguir, pelo tempo também. Imagina a cada 15 minutos uma medição,

se eu tentar medir 2 mil medições, eu vou ter dias, uma semana para fazer testes. Então a gente deixa isso por conta do operador quando ele quer fazer uma inspeção mais profunda em um determinado site ou em uma determinada configuração. Aí ele fiz: Ok, agora testa a comunidade tal, agora testa tal coisa. Não sei se te respondi, Fred.

SR. FREDERICO NEVES: Respondeu sim, obrigado, Leandro. Respondeu sim, obrigado. Tem mais alguma coisa, o Rubens tem mais perguntas.

SR. RUBENS KUHL: Teve uma dúvida, mas que estava respondida já no seu vídeo, que era sobre prepends negativos, e que a pessoa tinha entendido que seria mais do que dois. Mas não era isso, então talvez só repetir esse tema do prepend negativo.

SR. LEANDRO BERTOLDO: Prepend negativo foi um termo que até o... O pessoal conhece isso como prepend reverso também. Mas isso foi uma ideia do Prof. John, do sul da Califórnia lá, onde a gente faz... ele administra o root server B. Foi de fazer prepend em todas as outras instâncias, menos naquela. Então, tu mantém um único site sem prepend, e os outros sites, tu põe dois, três, quatro prepends. Porque o que a gente notou é o seguinte: se tu começar a dar muito prepend, teu prefixo acaba filtrado em algum momento. Então, coisas que a gente notou, assim, ah, tu deu dez prepends; ah, se deu dez prepends, teu AS-Path cresceu a um tamanho tal, que alguém está filtrando. Então, aí teu tráfego 'dropa' de, sei lá, 30%, que tu estava recebendo naquele [ininteligível] para algo em torno de zero, ou próximo disso.

Então, aí é que está o *takeaway* de que mais do que cinco prepends, a gente viu que era nocivo, três a cinco prepends, o efeito era praticamente nulo, e algum efeito a gente conseguia com um ou dois prepends. Algum efeito aí, a variação, se fosse negativo, até a 50% de tráfego; se fosse positivo, algo em torno de 7% para determinado site. Respondido, Rubens?

SR. FREDERICO NEVES: Tá joia, Leandro. Muito obrigado. Em nome do comitê do programa, eu quero agradecer. E, bom, a gente não tem palmas, ou nada, a gente encerra aqui. Um abraço.

SR. LEANDRO BERTHOLDO: Não. Muito obrigado, Fred. Valeu a oportunidade.

SR. FREDERICO NEVES: Até.

SR. LEANDRO BERTHOLDO: Até, tchau, tchau.

SR. FREDERICO NEVES: Muito bem, pessoal. Então, dando continuidade aqui ao GTER 49, agora a gente vai ter a próxima apresentação, Um ano de RPKI no Brasil, experiência e novidades no Krill. A gente vai ter o Alex Band, do NLnet Labs e, comigo também, um pequeno adendo. Alex, por favor.

SR. ALEX BAND (por intérprete): Estão todos me ouvindo? Maravilha. Eu vou, então, compartilhar a minha tela com todos. Vamos lá, então, eu sou o Alex Band. Eu trabalho no NLnet Labs. E nos últimos dois anos temos trabalhado com a autoridade de certificação através do Krill. E com base naquilo que construímos, nós começamos a conversa com o NIC.br porque eles queriam oferecer esse serviço de ARP para os seus associados, e esse foi o caso. Então, em dezembro de 2019 nós lançamos o Krill como um serviço, permitindo que todos pudessem fazer uma breve determinação de quem estava autorizado a conseguir fazer um roteamento de origem através do teu número AS.

Então, quem era o titular legítimo de um espaço IP e quem tinha essa autorização de conseguir fazer essa 'roteação' de um Sistema Autônomo? No momento, não havia um sistema disponível para isso. Nos últimos dez anos, outras partes do mundo tinham, sim, essa assistência disponível, mas não para o Brasil. Por isso, uma configuração específica era necessária, em que todos pudessem rodar aquele RPKI delegado. Na verdade, o que ele permite é que você possa, realmente, rodar a sua autoridade cientificada através de um registro internacional, que na verdade é um registro, uma certificação RPKI que pode ser internacional ou local. E o software, o Krill, que desenvolvemos faz exatamente isso, o que precisam fazer é simplesmente instalar e rodar. Daí você recebe um certificado e daí você tem um sinal através do teu CA pai. E daí você publica todos esses sinais e recebe uma definição.

A partir desse número AS, você pode originar esses prefixos. Qualquer um pode fazer o download dessa informação e pode fazer uma validação da rota, da origem da rota, que vai determinar quais recursos podem ser anunciados através de qual AS. A metas final é evitar o sequestro de BGP.

Esse gráfico é essencialmente aquilo que foi instalado em todo o mundo, o que temos disponível no momento. Os cinco registros globais, eles se estabelecem como *trust anchor*, que é um certificado de *trust*, e daí eles acompanham essa cadeia de *trust* permitindo que todos os certificados, eles possam estar relacionados a partir da tua rota de origem. E isso também pode ser feito através de outros recursos de internet.

Na maior parte das organizações e na maior parte dos casos pelo mundo, na verdade, há uma relação direta que os membros têm com o seu registro de internet regional. Mas este não era o caso ainda no Brasil, já que temos o NIC.br como o registro regional. Daí eles provém o serviço para vocês e nos permitem publicar isso através da sua própria infraestrutura ou o NIC.br faz isso por vocês. E essa é uma parte importe da infraestrutura que queremos construir. Internamente, todos esses certificados, todas essas rotas são publicadas em

diferentes bancos de dados em diferentes partes do mundo. Daí eles têm, aí, esse software que pode fazer o download, validá-lo e depois colocá-lo dentro do teu roteador, que são normalmente locais normais, você pode instalá-lo no teu RPKI.

No momento, eles estão introduzindo essa funcionalidade, na verdade, esse ano, primeiramente, como uma característica de base e depois de produção. E também oferecem outras soluções, como BGP, todos eles têm o suporte para o RPKI. Na verdade, é uma solução ponta a ponta, que funciona desde o registro originário da internet até chegando na parte final dos teus *routers*, em que você pode utilizar todas as declarações e todos os filtros. Os principais componentes aqui, que eu gostaria de apresentar-lhes é o Krill. A autoridade de certificado de RPKI, e que é uma publicação gratuita.

Nós lançamos, então, o Krill, como eu já disse, em dezembro do ano passado, juntamente com o NIC.br e eles provém o serviço. Para ser bem honesto com todos vocês, quando lançamos, eu já tinha experiência anterior com registros de internet regionais, eu e o Tim(F), meu colega, já trabalhávamos com o CCI. As pessoas estavam um pouquinho lentas nessa experiência, nessas operações, mas depois de um ano algumas pessoas já estavam tentando essa nova tecnologia, uma tecnologia surpreendente. E daí isso acabou excedendo os experimentos. Mas antes de eu chegar nisso, gostaria de colocá-los dentro de um panorama sobre quais eram os requisitos que o NIC.br tinha antes do lançamento do Krill, para entender quais eram as funcionalidades necessárias para que isso fosse lançado. A principal funcionalidade é para que pudesse ser operado, realmente, de maneira igualitária. Se você tem um ISP, que é baseado no endereço, por exemplo, o NIC.br ou o Lacnic, ou talvez de uma outra área, você pode rodar todos eles através de uma instância de Krill única e ver todos os endereços globais através de uma interface única. Você pode ter uma interação de um único IP. E nós queríamos oferecer isso de maneira, realmente, única para que as pessoas pusessem usar o Krill.

Internamente, vocês também poderiam agir como um CA pai para outras entidades, como, por exemplo, delegar a responsabilidade para uma das suas divisões ou para um dos seus clientes. E isso também estava embutido aí. É claro que com isso era necessário gerenciar esses ROAs, né, essas autorizações de origem de rota, e daí você se tornaria responsável por publicar esse material para o mundo. Ou ainda assim, você poderia delegar essa responsabilidade para terceiros, especialmente essa última parte aí, que é uma característica-chave para os membros brasileiros, porque eles podem instalar o Krill, mas eles apenas precisam garantir que eles vão atribuir os seus ROAs, e a publicação seja gerenciada pelo NIC.br, dando, realmente, um baixo limiar para o ecossistema, daí eles não têm que se preocupar com o servidor BGP e ficar rodando isso 24/7, tornando os ROAs

disponíveis para todo mundo. Eles não precisam se preocupar com os ataques de DDoS, porque os CAs pais vão se preocupar e vão cuidar dessas aplicações.

Para que as aplicações fossem mais úteis, nós pensamos: vamos precisar de alguns essenciais, e para que os limiares fossem os mais baixos, para que os parâmetros fossem utilizáveis. E para isso, nós podemos instalar o Krill a partir da sua fonte, o que é bem fácil, já que ele é programado dentro de uma placa, na qual é uma plataforma muito madura, muito fácil de ser utilizada. Nós temos os pacotes Debian, e Ubuntu, e também, se você quiser rodar no conteúdo Docker, também isso é disponibilizado. Nós queremos ter também uma interface de linha de comando, uma interface baseada na internet e também um HTTPS API e o REST-like. Dessa forma você consegue integrar facilmente na tua infraestrutura local.

E é claro, o monitoramento é essencial, e que ele possa rodar através de um alerta, uma indicação de qual efeito os seus ROAs estão sofrendo e quais as respostas de BGP que estão recebendo, não apenas localmente, mas pelo mundo, e também um log de auditorias, o que está acontecendo com os seus certificados no momento em que mudança é realizada no seu RPKI. Isso, então, se tornou disponibilizado logo no momento do lançamento, em 2019, e durante esse ano de 2020, nesses últimos meses.

Toda vez que pensamos em dar um passo além, as pessoas tinham que configurar tudo isso, rodar todas essas aplicações, talvez seria um pouco demais, não é? Estávamos pedindo além da conta. E estávamos, talvez, não atendendo às expectativas dos nossos usuários. E, talvez, uma coisa mais fácil. Então, tornamos o Krill disponível através do AWS e do mercado DigitalOean. A partir de um único clique, podíamos dar um *spin*(F), e o Krill, através do Wizard, ia, realmente, facilitar, liberar o certificado, te perguntar em que domínio você queria publicar os seus ROAs, ou em que domínio você queria atrelar, pôr como *host* o seu RPKI e daí você podia monitorar tudo a partir de um único clique.

Então, e dessa forma seria bem mais fácil, oferecendo soluções, e que apesar você paga pelo custo do VM e o software é completamente gratuito. Essa é uma boa maneira de tentar o software, experimentar o software, ter uma sensação de como você poderia monitorá-lo e depois, talvez, migrar para uma solução em que você pudesse fazer um *host* interno. E daí deixamos isso disponível por alguns meses e vimos que várias pessoas autorizaram para a outra plataforma. Interface de usuário, e essa interface de usuário seria uma interface não apenas em que clicasse para disponibilizar ROAs, mas também que pudesse dar sugestões, já que é uma instalação mundial. Nós pensamos que o suporte de múltiplas línguas seria importante,

incluindo o português do Brasil. No momento, temos seis idiomas incluídos, como o português brasileiro.

E a equipe de operações do NIC.br está nos ajudando com as traduções, então, toda nova versão, nós asseguramos que esses idiomas estão... que o original está traduzido para seis idiomas e o português brasileiro. O CA pai e também a configuração do servidor de publicação é feito através da publicação de terceiros que vocês vão rodar. Mas o mais importante de tudo, ele dá a possibilidade de sugestões de ROA e de alertas baseados nos coletores de rotas de BGP. Então, o que utilizamos é realmente os coletores para cada uma das atualizações de BGP que nós observamos através de todos os coletores de rota pelo mundo. Daí ele baixa e compara todos os prefixos que você tem no teu prefixo. E daí diz: Olha, esses são os endereços inválidos. Por favor, me quais desses prefixos estão autorizados e quais não estão. Todos esses anúncios são ditos como... e quais são os RPKIs inválidos, porque eles são originados a partir de ASNs incorretas ou porque eles têm um comprimento de prefixo incorreto.

Ele também cria um alerta sobre os ROAs permissivos, ou sobre ROAs redundantes. É assim que é a interface. Eu estou apresentando para vocês a versão em português, onde conseguem ver todos os anúncios que são feitos através dessa fase de ANSs(F), os endereços de ANSs(F). Nós temos aqui o ASP, que são anunciados, e também sobre os outros IPs, é outra infraestrutura de IOS IP. Aqui, os anúncios e as autorizações, os anúncios que são vistos e as autorizações. E também aquilo que não é anunciado. Isso pode ser, de repente, uma redundância, ou de repente uma invasão de rua.

Ao analisar os seus ROAs, ele vai te dizer: Olha, espera aí, você tem duas ROAs aqui, consulte as seguintes alterações, mas eu não vejo nenhum anúncio aqui, você, realmente, os quer aqui ou eu devo removê-los da lista? Ele realmente, sabe, vai te mostrando passo a passo, vai te guiando sobre qual é a melhor direção aqui ou no próximo passo, para que você, realmente, tenha a certeza na criação ou na manutenção dos seus ROAs.

Daqui para a frente nós passamos para a versão 1.0. E essa versão vai ter um API estável. E com certeza isso é o mais estável que queremos prover para os nossos usuários. Garantir que se você iniciar um programa contra o Krill dentro da tua infraestrutura local, que você não precisa realizar mudanças constantes conosco. Uma outra coisa que frequentemente nos perguntam é se necessário ter um suporte de múltiplos usuários, nós vamos criar isso a partir da funcionalidade OpenID Connect. No momento, o Krill, ele funciona com token master, é um token que você pode utilizar com a tua interface de usuário, a partir da configuração do arquivo. Com esse *config file,* tudo realmente é feito facilmente com todas as permissões disponíveis. Todos são

configurados como administradores, desde que você tenha o token, você pode fazer o que quiser. Daí você recebe um suporte, por exemplo, em que as pessoas apenas vão poder trabalhar como leitores ou ter a autoridade de suporte; outros que vão ter a capacidade da criação dos ROAs, ou aqueles que apenas vão ter a possibilidade de... o direito de leitura.

Todas essas funções serão possíveis a partir desse suporte de múltiplos usuários. Depois queremos criar suportes de *clustering*, uma lista de BGPs. Ao invés de utilizar dados de coleta, nós vamos usar... Espera aí que eu vou checar essa informação.

Ao invés de usarmos coleta de dados de *routers,* nós vamos usar dados que estão baseados na visualização do seu próprio *router*, e não dos coletores. Este é um diferenciador-chave de todas as outras soluções oferecidas no mercado, porque você vai ver exatamente aquilo que o teu *router,* que o teu roteador está vendo. E depois, essa... nós queremos suporte também para os HSMs, os módulos de segurança de hardware, ou seja, nós vamos implementar o PKCS #11 e o KMIP. E durante os próximos meses, nós vamos refinar essa interface do usuário através de logs, auditoria de logs, editar bulks e outras funções.

Então, como é que as coisas estão andando no Brasil? Eu já falei um pouquinho no início da minha apresentação, mas, na verdade, estão excedendo as nossas expectativas. O número das autoridades, dos certificados que foram autorizados nos últimos meses no Brasil, realmente, 500 quinhentos certificados. Além da qualidade dos ROAs criados, que é excepcional.

Vejamos aqui os dados comparados ao que foi anunciado, nós temos uma qualidade de dados que alcança 99% e mais de 2 mil ROAs que foram criados com o tempo. Para colocar isso dentro de uma perspectiva, no momento, 9.1% de todos os endereços estão cobertos pelo RPKI. Nossa, 9.1%? Mas, olha, isso é muito mais do que vários outros países nos últimos dez anos. Vocês fizeram isso em menos de um ano. Realmente, é impressionante. Vocês realmente devem se aplaudir e se parabenizar a respeito dessa porcentagem e da qualidade de dados que alcançaram em apenas um ano. É impressionante.

E talvez o ponto mais importante que eu gostaria de ressaltar aqui é o fato de terem alcançado e terem criado todos esses ROAs tem um efeito tangível nos *routers*, em si, na prevenção dos *hijacks* de BGPs, porque estamos vivendo um momento significativo em que as pessoas fazem essa validação através dos RPKIs em filtrar os seus roteadores, em que qualquer *hijack*, qualquer sequestro potencial de um prefixo que é originado a partir de um AS incorreto, ele é filtrado. Empresas como Telia, Cogent, GTT, NTT, Cloudflare, etc., etc. Todos fazem a filtragem através desses dados, então, se alguém anunciar o

teu prefixo através de um AS não autorizado, eles não irão propagar esses prefixos.

E este realmente é o ponto mais importante, eles não vão propagar esses anúncios. Então, com isso, eu vou deixar aqui o fato de que temos um ecossistema supervibrante no sistema. Aqui temos alguns links com toda a documentação, as perguntas mais frequentes, o GDR é uma ferramenta que te ajuda a explorar, inspecionar e ver todos os problemas, e que vocês podem, realmente, explorar. E temos também *webinars* que te ensinam o passo a passo sobre como empregar, validar dentro da tua rede. Eu editei, então, aqui esses links na apresentação. Vocês também podem acompanhar as contas no Twitter do Krill e nos seguir. E eu concluo. E agora eu passo a palavra para o nosso moderador para o resto da apresentação. Muito obrigado.

SR. FREDERICO NEVES: Muito bem. Vou falar um pouquinho sobre a nossa perspectiva em relação ao *deployment* do RPKI aqui no Brasil. A apresentação é do Kobayashi, do Alexandre Hamada. E vamos lá.

Bom, porque a gente trabalhou junto com o pessoal da NLnet Labs e a gente acreditava que esse modelo, o modelo delegado era o melhor modelo aqui no nosso caso. Bom, primeiro lugar, porque a gente acreditava, queria conseguir entregar junto com uma instituição tão competente como o pessoal da NLnet Labs um software de qualidade para esse *deployment.* Então, esse software foi entregue no ano passado, ele está consolidado e recebendo atualizações constantemente. Recebeu várias atualizações durante o ano, recebeu a interface gráfica Lagosta.

Então, do que a gente pode dizer e o que a gente tem monitorado é que para esses nossos 500 clientes, por favor, tentem manter o seu Krill atualizado, tá? Uma vantagem desse software é que os upgrades, mesmo se você tiver na versão 041, que foi a versão do *deploy* inicial, lá em dezembro de 2019, se você quiser fazer o upgrade para a versão atual, que é a 081, você pode fazer direto, sem ter que fazer upgrades intermediários, e vai funcionar, tá? Tenta manter o seu Krill sempre rodando, tá? Mesmo que ele seja utilizado poucas vezes, só para efetuar reassinaturas que ocorrem diariamente, ele precisa estar rodando o tempo todo. E se quiser utilizar o serviço de publicação do NIC.br, sem problema nenhum. Você pode utilizar e esse serviço é mantido com altíssima disponibilidade.

Bom, a evolução do Krill, como eu disse, a gente teve três principais upgrades aí, o 042, lá em dezembro de 2019, o 063, em junho, e o 081, agora, em novembro, com melhoras em relação, principalmente no 063, ocupando menos espaço em disco para CA, que chegou a ser um problema, no nosso caso, com muitos clientes CAs, sub CAs, conectados conosco. E no caso do 081, relacionada

principalmente à escalabilidade do serviço de publicação, o que pode não ser um problema para a maioria, mas no caso, acabava sendo um pequeno problema para a gente, mas isso já está solucionado.

Bom, em relação ao *deployment*, o sucesso desse *deployment*, a gente tem que citar claramente aqui o que o Alex apresentou na parte dele, é que isso só foi possível por causa dos treinamentos que o Ceptro tem feito. Então, além de a gente ter investido no software, e na implementação, a gente também investiu fortemente nos treinamentos. E em relação a isso, a gente tem que agradecer, e muito, o time do Ceptro, porque o RPKI foi incorporado no curso de BCOP, a gente teve seis turmas EAD de abril até novembro, total, 278 alunos, a gente tem uma próxima turma, agora, na semana que vem, infelizmente o curso já está fechado, mas a gente vai ter turmas, continuar tendo turmas no futuro. A semana de capacitação on-line, teve um evento específico para segurança no roteamento RPKI no dia 24 de agosto, e a gente teve mais de 6,4 mil visualizações, com pico de 817. Então, a gente olha lá no gráfico do *deployment*. E a semana de capacitação on-line é o que deu um grande *boost*, aí, vamos assim, no *deployment*. Mas se vocês olharem, a gente vem adicionando novos clientes desde o começo.

E a gente também teve eventos externos aí, um em relação à Revista RTI e também teve eventos fechados, aí, workshops, específico para o pessoal da Vivo e outro específico para o pessoal da Oi. E a gente continua tendo a possibilidade de efetuar esses workshops aí para turmas fechadas, quando necessário.

Bom, outra coisa é em relação à qualidade dos dados aí, e que o Alex citou, que os dados têm boa qualidade, mas isso se deve muito à questão da monitoração que a gente efetua aqui do lado do NIC. A gente começou a fazer isso ao redor de fevereiro e a gente faz checagens a cada uma hora e monitora todos os objetos RPKI publicados pelos nossos clientes. E a gente alerta esses clientes quando tem algum tipo de problema nesse repositório público, não é?

Bom, a gente faz o download desses objetos. Usando um software chamado software *relying party*, a gente usa o Routinator para isso. E a gente confere a questão da consistência dos arquivos de manifestos, dos ROAs, dos certificados, o que está publicado nas CRLs, e analisa, desses objetos, em relação à expiração, né, se ele não poderia ser usado antes de uma certa data, ou depois de uma certa data; qual é o update atual, qual o próximo update, não é? E também questão de hostnames inválidos. Se no prazo de uma semana um cliente não responder positivamente corrigindo um problema, a gente basicamente remove a delegação daquele cliente, o que faz com que os dados sejam bastante consistentes. E faz com que os clientes prestem bastante atenção em relação a essa monitoração.

Bom, os avisos. No painel também, na interface de delegação do sistema de registro, a gente também provê essa informação, se existe algo inconsistente ou não, não é? Bom, em relação ao *deployment* aí, a gente tem um pequeno gráfico aqui, mostrando os 534 CAs que a gente tem delegados atualmente. Então, a gente tem 128 em São Paulo, 77 no Rio, 55 em Minas, 33 Pernambuco, 32 no Paraná, mas tem *deployments* praticamente no Brasil todo. Em relação à porcentagem aí, a gente tem 6,3% dos titulares de endereçamento IP já cobertos aí, sendo que a maior cobertura que a gente tem hoje é no Rio de Janeiro, com 13%.

Isso daqui é uma estimativa de quem está utilizando e está validando ROAs aqui no mercado brasileiro, e a gente faz isso baseado nas conexões que a gente recebe no serviço de publicação. E olhando só para os endereços brasileiros aqui, a gente consegue ver que ao redor de 4,3% dos IPs que usam rsync foram aqui... são de instituições que estão no Brasil. E a gente tem aí essa quantidade de *relying parties,* ou seja, organizações que estão se utilizando dessa informação de roteamento segura para aceitar esses prefeitos aqui no Brasil, que é bastante bom. A gente está vendo que isso está crescendo, o que é muito positivo.

Bom o que a gente vê como vantagem do modelo distribuído de RPKI, não é? Primeiro lugar, a gente tem um ecossistema bastante robusto em relação ao que o Alex falou, dos requisitos iniciais lá para software. A gente conseguiu entregar tudo isso. E uma outra coisa muito interessante que pode passar despercebido, mas tem muita organização que está presente em múltiplos países, e usar o modelo hospedado, não o modelo delegado, pode parecer mais simples em um primeiro momento, mas você acaba tendo que ir para uma organização que está em múltiplas localidades, você acaba tendo que gerenciar múltiplas interfaces, sendo que com o modelo delegado e com um software como o Krill e a interface que ele tem, você pode gerenciar isso tudo em um único local. Outra questão é que a responsabilidade pela manutenção do material criptográfico da sua instalação é sua e exclusivamente sua. Esse é um risco que, no modelo hospedado, ele é transferido para a organização que efetua isso. E no caso de fornecer um atestado de... assinado criptograficamente de quem pode originar os seus prefixos, é algo bastante delicado. Então, esse foi um dos motivos principais para a gente ter optado pelo modelo delegado e totalmente distribuir.

Bom, a gente está fornecendo os treinamentos gratuitos e pretende continuar fazendo isso. A gente tem uma equipe dando suporte. E também a gente tem essa questão de estar disponibilizando o software e mantendo ele de forma atualizada e ajudando que essa manutenção seja efetuada. Bom, e, de novo, a gente gostaria muito que você começasse a usar RPKI, tá? Então, se você é um dos oito,

dos outros 8 mil Sistemas Autônomos aqui no Brasil e que ainda não está usando, por favor, use.

Então, era isso o que eu tinha para contar, um pouquinho da história de um ano de RPKI no Brasil. A gente ainda tem muito para fazer, mas eu acho que a gente está no caminho certo. E eu gostaria de abrir para perguntas. Se Rubens puder coordenar isso, eu agradeço.

SR. RUBENS KUHL: Obrigado, Alex, obrigado, Fred, pelas apresentações. A pergunta que a gente tem é do Hugo Salgado, do NIC CL, ele pergunta se poderiam usar o Krill sem uma delegação de autoridade certificadora, para usar só os recursos de monitoração, sem necessariamente aí se envolver no processo de ser uma CA e assinar aí um recurso de mineração.

SR. ALEX BAND (por intérprete): Querem que eu responda essa pergunta? Teoricamente, sim, isso é possível. Poderia, por exemplo, usando o *testbed* que nós oferecemos, você pode, na verdade, designar qualquer recurso que queira. E com isso você consegue monitorar o que disse com relação aos recursos. Mas preciso dizer que é a primeira vez que eu ouço uma solicitação desse tipo, porque a maior parte das pessoas querem usar como, por exemplo, um alerta de BGP, que é uma solução aberta para fazer quase que a mesma coisa. E a gente também pode usar para, também, fazer um alternador de IP, para você validar em um *endpoint*, desde que você tenha um prefixo e um número AS, para entender qual é a validade.

E usando essas informações, a gente poderia também ter essa característica de alerta. Então, usar o Krill com um *testbed* e usar também falando com o alternador de IP. Seriam algumas das opções para responder a isso.

SR. RUBENS KUHL: Por enquanto, a gente não tem mais perguntas. Então, só dá um tempinho para o pessoal pensar um pouquinho, mas se não, a gente vai encerrar.

SR. FREDERICO NEVES: Bom, eu vou aproveitar enquanto não chega nenhuma pergunta. Eu gostaria de agradecer publicamente aqui o Alex pela colaboração que a gente tem tido com o NLnet Labs, tem sido muito frutífera. Ela já é mais antiga. Nós utilizamos software deles para provisionamento DNS, o NSD, e também um software para a validação do DNSSec Unbound, mas a experiência que a gente tem tido, agora, com o *deployment* de RPKI só vem estabelecer melhor esse vínculo que a gente tem com a organização. Eu gostaria de agradecer eles publicamente aqui por toda a competência e a parceria que têm tido conosco, com a nossa equipe de engenharia.

SR. ALEX BAND (por intérprete): Ah, de nada. Eu também gostaria muito de agradecer pela cooperação técnica, por tudo o que tem feito para aumentar o alcance e também a contribuição financeira,

o investimento, para que nós possamos oferecer este trabalho. Com certeza, são excelentes parceiros. Muitíssimo obrigado a todos também.

SR. FREDERICO NEVES: Algo mais, Rubens?

SR. RUBENS KUHL: A gente tem uma pergunta agora, uma pergunta do Gleisson Ramos(F) que é: o que acontece quando não for validado no Krill o site ou o IP. Eu imagino que ele estaria perguntando o que acontece se falhar uma validação, mas talvez com dois ângulos, né, de: se existe uma ROA e se não existe uma ROA.

SR. ALEX BAND (por intérprete): Querem que eu responda? Primeiro, vamos ver se eu entendi a pergunta corretamente. Um Roa, ele vai dar essa intenção, não é? Desde que você tenha uma ROA autorizando o anúncio, ele vai considerar válido. Mesmo que a gente tenha um ROA conflitante que torne isso inválido, não importa, você pode ter dez ROAs que tornem inválido, mas se você tiver um que autoriza, tudo bem. Não tem problema algum.

E outra parte, se a validação não for mais possível, aí tudo vai voltar a basicamente naquele status não encontrado, como se o RPKI não fosse usado. Mas se você tiver que tomar uma decisão de roteamento, aí, sim, ele vai aceitar tudo o que for válido. Aí você vai automaticamente rejeitar aquilo que for inválido. Mas também deveremos aceitar aquilo para o qual a gente não tem nenhum *statement.* Provavelmente, a gente nunca vai chegar em um ponto onde você tem 100% de *deployment* e cada anúncio, em todos os lugares do mundo, vai ser coberto pelo RPKI. A gente não vai chegar nesse momento onde a gente vai também rejeitar algo que não foi encontrado ou que está naquele status desconhecido.

Então, para resumir, o RPKI, ele falha, mas de maneira segura, desde que você tenha um anúncio positivo, desde que você tenha isso, aí você pode tomar uma decisão de roteamento.

SR. RUBENS KUHL: Obrigado, Alex. Obrigado, Fred.

SR. FREDERICO NEVES: Mais algo, Rubens?

SR. RUBENS KUHL: Não [ininteligível].

SR. FREDERICO NEVES: Então tá joia. Então, com isso, a gente encerra aqui a última apresentação do GTER 49, primeiro dia da 10ª Semana de Infraestrutura da Internet no Brasil.

E, em nome do Comitê de Programa, eu gostaria de agradecer a todos os apresentadores, ao público que está nos acompanhando desde as 9h da manhã. E o nosso muito obrigado. E retornamos amanhã às 9 horas para o GTS.