SR. EDUARDO BARASAL MORALES: Bom dia, pessoal. Sejam todos bem-vindos aí a nossa Live Intra Rede, a live que a gente sempre tenta trazer um pouco das discussões sobre redes e infraestrutura que estão acontecendo aí no dia a dia dos sistemas autônomos. E no dia de hoje, a gente vai ter uma live sobre segurança na Internet, e qual é o nosso papel, e aí a gente trouxe representantes de cada um dos setores aí que acabam compondo a Internet para ele dar o quê? Uma visão do setor dele, de qual é a responsabilidade na questão de segurança. Então, a gente vai ter uma pessoa que vai estar representando conteúdo, representando aí as pequenas prestadoras de telecom, pequenos provedores, as grandes operadoras de telecom, vamos ter ali um representante dos fabricantes, um representante aqui do NIC.br como uma instituição neutra, vamos ter ali também representante do governo, tá? Então, a gente quer trazer nessa discussão quais são os papéis de cada um para a gente ter uma Internet melhor para todos, uma Internet mais segura, tá?

Mas antes da gente começar a nossa live, como já é de praxe, eu queria agradecer os nossos patrocinadores. Então, é Juni Link IP & Cloud Network by GIOVANELI Consultoria, WZTECH Networks, ICANN, Netfinders Brasil, Novatec Editora, Eletronet, GlobeNet Telecom, Mundivox, 4Linux, Solintel, Cisco e Logicalis, 4Bios IT Academy, Globo, Netflix, FiberX e Huawei, e o apoio de mídia da revista RTI e Infra News Telecom.

Para aqueles que quiserem o certificado dessa live, vocês podem se inscrever no link que está sendo colocado agora no chat do Youtube, e depois que você clicar nesse link e se inscrever lá no nosso site, tem que ficar atento ao e-mail, porque vai ser enviado um e-mail para você, e até às 14h você tem que clicar no link que vai nesse e-mail que é para confirmar que você está assistindo a live aqui com a gente. E aí, você vai ganhar o certificado depois disso. Então, presta atenção: precisa se inscrever no link que o pessoal está colocando no chat agora e olhar o e-mail, porque tem um link lá para confirmar que você está assistindo, tá? E isso é até às 14h.

Temos também, pessoal, sorteios, não é? Então, como já é de praxe, toda live a gente tem aí um sorteio para fazer, e aí a gente tem o quê? Quatro sorteios hoje. Então, o primeiro deles é do NIC junto com alguns patrocinadores, é um kit de prêmios, tá? Então, vai ser uma caneca da ICANN, um kit de acessórios para vinho da Cisco, uma caixinha de som a prova d'água da Cisco, um kit da Moleskine e caneta da Logicalis, um voucher da Globoplay de acesso para dois meses da Globo, um livro Vida de Programador - Volume 0 da Novatec Editora, um livro Vida de Programador - Volume 1 da Novatec Editora, uma garrafinha de alumínio mais uma caneta personalizada da Juni Link IP & Cloud Network by GIOVANELI Consultoria, uma camisa polo da Semana de Capacitação do NIC.br, uma lapiseira da Semana de Capacitação e um kit de adesivos individuais de IPv6, RPKI, do NIC.br.

Então, é um kit aí, depois a gente vai mostrar para vocês, vai tirar uma foto, o Moreiras já até está montando ali atrás dele todas as coisas que vêm nesse kit para vocês verem o que vai ser o presente do sorteado, tá? Para participar, precisa se inscrever no link que o pessoal está colocando agora no chat. Agora os outros sorteios: tem o da Netfinders Brasil, que é uma vaga no curso BGP e MPLS Avançado em Huawei - modo gravado, tá? Então é um novo link que precisa se inscrever. GlobeNet Telecom está sorteando ali um fone de ouvido sem fio Bluetooth, tá? E no formulário, pessoal, é importante ver que é só e-mail corporativo, tá? E temos também o sorteio da Globo, que é um voucher de acesso grátis por dois meses da Globoplay, tá? Então, esses são os sorteios, são quatro sorteios, são quatro links aí para você se inscrever, não deixa aí de participar.

Agora, pessoal, eu gostaria de chamar o videozinho do Cidadão na Rede, lembra? É uma iniciativa nossa, de a gente querer trazer ali uma informação para o nosso usuário comum, como ele ser um bom cidadão digital, um bom cidadão na Internet. Então, a gente faz esses videozinhos, a gente gostaria do apoio de vocês para divulgar essa ideia. É uma maneira de que vocês possam pegar esses videozinhos, colocar o logo de vocês. Basta se inscrever lá no site do Cidadão na Rede, baixar e colocar nas redes sociais de vocês, fazer um marketing digital. É um jeito de fidelizar os seus clientes. Então, a gente quer o quê? Disseminar esse conhecimento. Esses videozinhos não são para grandes pessoas técnicas, grandes pessoas com alto nível de conhecimento, mas são para aquele usuário comum, que não sabe direito ainda como a Internet funciona, não está sabendo como se portar na Internet. Tem até um pouco ali aquela questão de achar a Internet um lugar inseguro, porque, às vezes, vem muito link, tem muita coisa para clicar, tem muita gente ali fazendo coisas ruins. Então, esses videozinhos, a gente aborda várias questões de ser um bom cidadão na Internet, e a gente precisa da ajuda de vocês para divulgar esse conhecimento. Então, eu vou pedir para tocar o videozinho agora. Pode tocar.

[exibição de vídeo]

SR. ANTONIO MARCOS MOREIRAS: Gente, muito bom dia a todos e todas que estão nos acompanhando, acompanhando mais essa Live Intra Rede do NIC.br. Sejam realmente muito bem-vindos. E eu gostaria de saber de vocês aí como é que está, antes de a gente chamar os painelistas e começar realmente a tratar do assunto do dia, como é que está a transmissão? O som está chegando legal para vocês? A imagem está com boa qualidade? Lembra que essa live está sendo transmitida pelo Youtube, onde eu acho que a maioria do pessoal está assistindo aqui, mas a gente também tem as transmissões ao vivo pelo Facebook e pelo LinkedIn, que é uma novidade aí. Se alguém

quiser acompanhar lá e ver como é que está isso, ou gostar mais de uma plataforma ou de outra, escolham a plataforma que mais lhes agradar aí, não é? Normalmente, a gente faz as interações aqui, o pessoal está se concentrando um pouco mais aqui no Youtube. Muito bom. O pessoal está falando que o som está legal, que está tudo bem. Alguém está reclamando que a imagem está um pouquinho tremida, o André. Onde é que está tremida, André? Está tremida... a imagem está bem tremida? Está tremida no Youtube mesmo? Vamos dar uma olhadinha nisso aí. O pessoal técnico já está aqui, então, ciente disso e vai dar uma olhadinha para ver se a gente consegue melhorar. Muito obrigado aí pelo... mas vamos melhorar. O som pelo menos está chegando limpo. Então, desculpem se a gente tem algum probleminha técnico com imagem, o pessoal está tentando dar uma olhada aí. Para algumas pessoas, parece que está chegando tremida, para outras, não. Então, a gente vai ver o que está acontecendo. Mas o som está chegando limpo, também isso é a parte mais importante. Temos aí também a estenotipia ao vivo, as legendas, que ajudam a gente a entender. Então, daqui a pouquinho a gente vai chamar já os palestrantes, os painelistas.

E como as nossas lives no geral aqui, a gente vai dividir em dois momentos principais. A gente chama primeiro os painelistas, a gente tem aqui hoje com a gente o Eduardo Parajo, da Durand Tavola, representando os provedores de Internet e os pequenos prestadores de telecomunicações; a gente tem o Paulo Martins, da Claro, e o Cristiano Pimenta, da Claro, representando as empresas de telecomunicações, as grandes empresas de telecomunicações, os grandes provedores de Internet; o Fernando Zamai, da Cisco, falando pelo setor aí de fabricantes; a Vanessa Copetti Cravo, da Anatel, falando pelo regulador; o Alê Borba, do Google, falando também aí como... representando o setor aí de conteúdo, serviços na Internet; e a Cristine Hoepers, aqui do próprio NIC.br, do CERT.br representando a comunidade técnica, os especialistas em segurança.

E esse tema, realmente, é um tema muito importante, muito legal, a gente vê que está sendo muito discutido, e, hoje, a gente quis justamente abrir esse espaço para cada setor vir e dizer qual é o seu papel, como é que cada setor tem contribuído e pode melhor contribuir para a segurança na Internet. A Internet é uma construção coletiva, é uma construção de todos, mas muitas vezes a gente quer, vamos dizer assim, que... quando a gente fala de segurança ou quando a gente fala de vários outros temas, a gente fica achando que, ah, todo mundo tem que fazer isso, todo mundo tem que fazer aquilo, e, às vezes, os diferentes setores podem ter papéis diferentes, limitações no que podem ou não podem fazer. Então, justamente para saber de cada setor, de cada tipo de empresa, qual a sua visão sobre isso, foi o que a gente organizou esse evento, essa live. E vocês que estão nos acompanhando aí, eu imagino que muitos já tenham vindo... tenham

acompanhado lives anteriores, já sabem da qualidade do conteúdo que a gente traz aqui. Então, deem um voto de confiança para a gente, deixem já o seu *like* no Youtube ou na plataforma que estiverem acompanhando, porque isso é importante para a gente. A gente confia muito na distribuição orgânica, naquele aviso que o Youtube mostra aquele vídeo para as outras pessoas para lembrar que isso está acontecendo, para lembrar... depois o vídeo fica gravado na plataforma, para lembrar que tem aquele vídeo para o pessoal poder acessar o conteúdo. Então, quanto mais *likes* tem o conteúdo, para mais gente ele chega, e é um conteúdo que a gente sabe que é importante, sabe que vai ajudar muita gente. A gente sabe que vai ajudar a entender melhor a Internet e todo o contexto que a gente está vivendo hoje. Então, o *like* de vocês é uma contribuição muito, muito importante para a gente.

Bom, vamos lá. O pessoal está dando uma dica aí no chat, quem está vendo tremido, para baixar a qualidade para 720p ao invés de ver em *full HD*. Pode ser. Quem ainda estiver com problemas na transmissão, vendo a imagem um pouco tremida, pode tentar fazer isso. Vai lá na própria... no próprio Youtube ali tem no vídeo aquela engrenagenzinha, e muda lá a qualidade de reprodução para uma qualidade... não para o 1080p, mas coloca lá 720p ou 480p, que o pessoal... tem um pessoal aí no chat dizendo que pode melhorar... melhora a tremedeira da imagem se fizerem isso. Então, a gente... do nosso lado aqui, a equipe técnica está trabalhando nisso, mas vocês podem experimentar aí do seu lado também fazer esse pequeno ajuste, que, segundo o Henri, algumas outras pessoas que estão aí no chat colocando *reports*, isso ajuda.

Bom, gente, sem mais delongas aqui, sem... eu vou chamar. Então, como eu dizia antes, vai ter dois momentos. Agora eu vou chamar os painelistas, cada um vai ter em torno de dez minutos para apresentar a visão do seu setor, e eu e o Eduardo vamos chamando. Depois, quando todos fizerem essa apresentação inicial, aí a gente vai partir para a parte das perguntas. Então, se vocês, durante as apresentações, tiverem questões, vocês vão colocando aí no chat, a nossa equipe está anotando tudo, e depois, na medida do possível, na medida que o tempo permitir, a gente vai, na segunda parte, colocando essas questões, seja para um painelista individual, seja para a Mesa inteira, para todos de uma vez, conforme a questão pedir, não é E também depois, se algum painelista tiver questões para o outro, ele também vai poder fazer nessa segunda parte, enfim.

Bom, gente, tem gente aqui dizendo que a qualidade... que o tremido ainda está persistindo, mesmo com a qualidade baixa, mesmo baixando, vamos dizer assim, a resolução do vídeo, vamos dizer, o tremido ainda persiste. O que a gente tem a fazer aqui... a gente vai seguir, a gente vai seguir o conteúdo. Eu estou, pelo menos, entendendo de vocês que o áudio está legal, é o mais importante, não

é, que a gente ouça o que cada um tem para falar. Peço desculpas, a gente não sabe ainda a razão disso, a nossa equipe técnica está aqui trabalhando para tentar melhorar esse problema. Espero que consigamos, mas se não conseguirmos, sigamos assim, porque o conteúdo em si é muito importante, o áudio, o que as pessoas vão falar é muito importante.

Então, vamos seguir com isso. Vamos seguir com a live, e eu vou abrir agora para o primeiro painelista, que é o Eduardo Parajo, da Durand Tavola. Eduardo Parajo, por favor, então, tome aí... o palco é seu, tome a palavra e siga com a apresentação.

SR. EDUARDO PARAJO: Obrigado, Moreiras. Bom dia a todos. É um prazer aí estar participando mais uma vez dessas lives do Intra Rede. Parabéns aí para o NIC pela iniciativa, sempre muito bom, trazendo assuntos relevantes. Queria cumprimentar também os outros painelistas e aproveitar para trazer aqui um ponto com relação a essa questão da segurança da Internet, que é o nosso tema principal hoje, e falar qual é o nosso papel. Eu sou Eduardo Parajo, para quem não me conhece, tenho uma empresa, que é a Durand Tavola, e também faço parte da Abranet, faço também parte do conselho do NIC, e estou nesse mercado aí desde os primórdios, não é? E nem vamos falar muito das datas para não ficar chato e a gente revelar quantos anos nós temos, né, mas já está há um bom tempo.

Eu vou falar um pouquinho do lado dos provedores de Internet, das pequenas prestadoras, o que o pessoal tem feito em geral com relação a questões de segurança e para deixar a nossa Internet cada dia melhor. Do lado dos provedores em geral, a gente, obviamente, tem sofrido e passado aí por diversas intempéries de segurança nesses anos todos e nesse processo todo, onde, obviamente, a gente convive desde problemas, sei lá, de vírus, ransomware, problemas de ataques DDoS e tudo o mais, não é? E os provedores, em geral, têm tomado medidas para que possam estar efetivamente protegendo aí a sua infraestrutura, a sua rede em geral, todos os seus servidores e tudo o mais, e têm tem atuado de forma, eu diria, bastante forte nessas questões. Um dos projetos aí que eu poderia elencar nesse momento são as próprias referências aí do site NIC e do BCP, daquelas recomendações do MANRS, onde a gente, com poucas, vamos dizer assim, correções na rede, na questão dos equipamentos, melhora aí a questão de poder sofrer ataques, ou refletir ataques para a Internet como um todo a partir dos seus provedores, e, evidentemente, que cada dia mais essas empresas estão preocupadas aí com a sua segurança no geral e a dos seus usuários para que eles possam ter sempre a conectividade, não é?

Uma outra questão que eu acho que é importante destacar nesse sentido é também a participação dessas empresas em geral nestas campanhas de segurança para os usuários. A gente sabe muito bem

que hoje os maiores problemas que a gente encontra, normalmente, eles acontecem a partir dos usuários que têm as suas máquinas aí não configuradas adequadamente, ou por falta de atualizações de software, por falta de proteção de antivírus, esse tipo de coisa, e essas máquinas normalmente acabam sendo remotizadas e utilizadas de forma indevida e acabam, infelizmente, propagando os ataques para a Internet como um todo, ou servem de refletores para a Internet como um todo. Então, a gente tem apoiado bastante essas campanhas e tem divulgado bastante os vídeos aí do NIC sobre segurança, o que realmente acaba... parece que é uma coisa pequena, mas quando você reflete isso para muitos computadores ou muitos usuários espalhados pela Internet como um todo, isso acaba trazendo uma grande proteção de formiguinhas, vamos dizer, mas esse monte de formiguinha junto acaba ajudando a Internet brasileira como um todo, não é?

Fora isso, eu vejo vários também provedores hoje com ações educativas, como eu falei, na questão... junto aos seus usuários, fazendo um trabalho forte aí para que esses usuários tenham as suas proteções e tenham todo esse processo e, evidentemente, que aí cada provedor tem tomado, vamos dizer assim, providências para proteger a sua conectividade, proteger elas de ataques externos, proteger a sua infraestrutura e deixar isso cada vez mais seguro. Evidentemente que a Internet, a gente sabe, é uma coisa bastante complicada, tem gente que está usando a Internet de forma adequada e para o bem e sempre também tem aquelas pessoas que acabam utilizando a Internet de maneira, vamos dizer assim, prejudicial para a Internet como um todo. E a gente tem acompanhado isso de forma diária, quase que horária, toda hora a gente vê essa situação acontecendo, e obviamente que a gente tem que utilizar contramedidas nesse processo.

Tem também uma questão importante que eu acho que é relevante comentar, que são os próprios provedores que têm, de certa maneira, trocado muitas ideias e muitas experiências entre si nessas atividades, não é? Quer dizer, os provedores acabam se comunicando entre si aí, falando um pouco entre eles sobre medidas, e situações, e formas que eles têm reagido, principalmente com relação a ataques DDoS, que é, vamos dizer assim, uma parte que acaba afligindo bastante os provedores e acaba prejudicando bastante, tem se conversado para trocas de experiências nesse processo como um todo, e isso tudo é de uma forma bastante contributiva, vamos dizer assim, contribuindo para a Internet, contribuindo para esse bem-estar da Internet e contribuindo aí para a segurança da Internet no Brasil.

É importante também destacar que boa parte das... aí eu vou separar um pouquinho, falar um pouco das prestadoras de telecom, tem as suas medidas, as pequenas prestadoras têm suas medidas e têm tomado todas medidas para proteger a infraestrutura de telecom que dá suporte aí para a conexão de Internet, mas, evidentemente, que a gente tem que também lembrar que nós estamos falando em

pequenas, micro, médias empresas espalhadas pelo Brasil todo, e essas médias e pequenas empresas têm as suas dificuldades no sentido de manter, vamos dizer, essa infraestrutura e, obviamente, de proteger também essa infraestrutura. Eu acho que, assim, o importante de a gente também destacar é que esse lado colaborativo da Internet como um todo acaba facilitando um pouco esse processo, porque a gente sabe que efetivamente não existe aí, vamos dizer assim, braço e recurso suficiente para cada um colocar, vamos dizer assim, as suas trincheiras aí, não é, muita gente nesse processo que acaba efetivamente encarecendo demais as operações, mas aí, com esse lado colaborativo, vamos colocar dessa forma, e essa contribuição entre os provedores e tudo o mais, ajuda como um todo.

E aí, eu gostaria de destacar também o papel do NIC, não é? O NIC tem feito um trabalho muito interessante de divulgação e de práticas, de boas práticas, na adoção de boas práticas para os provedores, que isso facilita e traz mais conhecimento para esses provedores, não é? Então, de fato, aí eu poderia dizer para vocês que os provedores em geral, eles têm estado muito atentos a essa questão de segurança, têm tratado isso de forma bastante prudente e com bastante atenção, porque sabem que se der brechas ou criar... vamos dizer assim, tiver problemas, não é, isso pode afetar não só a infraestrutura dele, mas aí milhares de usuários que estão conectados utilizando a Internet dele. Então, esse trabalho que eles vêm fazendo é muito importante, é de forma, na sua grande maioria, de forma voluntária, não é, eles se interessam em estar fazendo esse tipo de trabalho, e eu acho que dessa forma aí, com o apoio do NIC, com o apoio de outras entidades, para que eles possam efetivamente estar colaborando e ajudando a nossa Internet a ficar cada vez mais segura.

O MANRS, só falando desse projeto, acho que foi uma coisa muito interessante. Essas boas práticas que têm sido colocadas pelo NIC ajudaram muito os provedores a configurarem melhor os seus equipamentos, configurarem melhor os equipamentos que estão colocados nos usuários, fazerem uma trava de proteção um pouco melhor na sua rede para que ele não possa refletir, e eu acho que a gente tem que efetivamente continuar propagando e fazendo bastante barulho sobre essas questões junto aos provedores para que a gente possa, efetivamente, dar uma proteção melhor para a Internet no Brasil.

Eu acho que esses são os meus comentários iniciais aí, Moreiras. Obrigado, Eduardo, pelo convite, e fico à disposição aí para perguntas.

SR. EDUARDO BARASAL MORALES: Obrigado, Eduardo Parajo. Realmente muito interessante tudo o que você falou.

E, agora, eu gostaria de chamar o nosso próximo palestrante, que é o Paulo Martins, da Claro. Então, Paulo, fica à vontade, o palco é seu.

SR. PAULO MARTINS: Bom dia, pessoal, todos que estão assistindo pelo Youtube. É uma excelente iniciativa do CERT.br. Como o Parajo acabou de ressaltar muito bem, a Internet, ela é para todos. Então, nós temos uma questão aí muito... uma responsabilidade muito grande, que é prover tudo e toda a Internet de uma forma segura e permitir que pessoas com níveis diferentes de conhecimento, de tecnologia, possam usufruir todos os serviços que têm para a Internet. Eu vou compartilhar uma pequena apresentação, alguns slides, só para a gente poder usar, para relembrar alguns papéis, que são os papéis das grandes Telcos e dos provedores em geral. Obviamente, inclui também os provedores pequenos, não só as grandes Telcos, mas os provedores também.

Durante a live, infelizmente, eu não vou conseguir ficar todo o tempo. Está comigo aqui o Cristiano Pimenta, e o Cristiano vai estar o tempo inteiro aqui. Ele é o gerente de segurança corporativa da Claro. Então, ele vai estar aqui. Para quem não me conhece, eu estou no grupo claro já tem três anos e eu sou o responsável pela segurança corporativa da Claro no Brasil, tá?

Então, qual é o papel das Telcos? Primeiro: existe todo um arcabouço jurídico, e todas as Telcos, elas são reguladas pelo regulador, que é a Anatel. Inclusive, a Vanessa está aqui, depois ela vai expor um pouco papel do regulador. E nesse ciclo todo da Internet tem algumas leis que estão em vigor para poder pôr algum direcionamento ou ter alguma possibilidade para, quem se sentir prejudicado, poder reclamar em um órgão específico. Então, existem 17 delegacias de crimes cibernéticos, a primeira foi criada em 2010 no Rio Grande do Sul, mas, como vocês podem ver, nem todas as unidades ainda têm uma unidade... nem todas as unidades federativas, ou seja, os estados, têm ainda uma delegacia. Tem uma lei de 2012, que ficou conhecida como Lei Carolina Dieckmann, que é sobre a questão de exposição na Internet, exposição não consensada (sic), então é uma lei que está em vigor desde 2012; tem o Marco Civil da Internet, que também regula como é que é o tratamento dos tráfegos na Internet, então é uma lei de 2014; e mais recentemente entrou em vigor a lei... a LGPD. Então, existe todo um arcabouço aí jurídico para... que regula toda essa interação pela Internet.

Qual é o grande papel das Telcos? É fornecer os caminhos para a Internet. Então, as Telcos, elas não têm a responsabilidade de bloquear ou impedir por fragilidade de ética ou conduta dos usuários. Então, ela é um caminho, e a responsabilidade do que está circulando é do cliente, é do site, não é... A Telco, o papel dela é realmente prover o acesso, prover o caminho que vai ser usado. A gente tem, em alguns casos, tem uma Lei de Quebra de Sigilo Telemático, que é quando alguém se sente prejudicado ou há um crime, então a autoridade policial, a autoridade judiciária, através dessa lei, ela pode pedir a quebra do sigilo telemático de algum usuário ou de algum provedor.

Então, é uma lei que existe e tem essa conotação aí, tá? E nesse caso, a gente tem uma obrigação, então as Telcos e todos os provedores têm uma obrigação de fornecer as informações de conexão, e se for no caso de quebra de... interceptação telemática, transferir esse tráfego, copiar esse tráfego para a autoridade, tá? Agora, as Telcos elas não armazenam nem as conversações, nem os SMSs, nem os dados que foram trafegados, o que ela tem obrigação de ter é quem ligou para quem, que hora que foi, quanto tempo durou, esse tipo de informação que é o que tem com as teles, tá?

Uma questão que tem aparecido que até está sendo cunhado um termo, chamado *smishing*, que é o spam de SMS, que é uma questão importante aí, porque ele acaba... ele pode ser usado de forma indevida. Então, é o uso indevido do *short code message*. E não temos ação nas fraldes e golpes de mensagens instantâneas e redes sociais. Então, eu tive problema com o meu WhatsApp, alguém criou um outro WhatsApp, pôs minha foto e está se passando por mim. Isso está à nível da aplicação, não está à nível da responsabilidade da Telco, que é fornecer o caminho, tá? Então, é um tipo de golpe que tem acontecido bastante. E aí, na linha do que o próprio Parajo estava colocando, tem uma parte educativa muito grande, e isso, sim, é responsabilidade das Telcos, porque a gente tem uma quantidade muito grande de clientes finais. Então, nesse caso, nos casos que... de educação, é uma responsabilidade e é um papel que a gente tem feito de prover a informação de forma clara, inclusive os cuidados, para os clientes.

Então, a gente tem feito campanhas direcionadas. Isso todas as teles têm feito, não é uma questão só da Claro, tá? No caso da Claro, no próprio site tem, na aba Segurança, uma série de dicas para os usuários da Internet. Agora, todos os atores envolvidos, eles têm que estar engajados nas boas práticas e na ética do uso da Internet. Então, a Internet, ela vai ser só as vantagens que tem essa conectividade em todos os lugares e conteúdos dos mais diversos possíveis se a gente tem as pessoas, os atores todos seguindo as boas práticas e a ética do uso da Internet.

Aí são algumas dicas que, por exemplo, a gente tem propagado bastante para todos os clientes, e as Telcos, em geral, têm colocado isso para todos os clientes. As Telcos e os provedores, porque essas são boas práticas em um linguajar o mais próximo possível do usuário leigo para poder ajudar nessa questão de transformar a experiência no uso da Internet uma experiência agradável, uma experiência interessante. A primeira questão: manter os recursos de segurança habilitados e configurados. Não adianta, por exemplo, dentro de uma rede social ela ter os recursos e a gente não usar, porque aquilo vai ser... pode ser usado contra a gente. Trocar senhas, e não colocar coisas fáceis do tipo assim: Paulo123. Pô, se o meu nome é Paulo... e 123 é uma senha muito simples de ser quebrada. Então, é uma senha que eu não deveria jamais usar, a Paulo123. Não clicar em links

desconhecidos, nem cadastrar os dados pessoais e bancários em qualquer site, tá? Muito cuidado onde está sendo colocada essa informação. Cuidado ao que se publica nas redes. A rede, ela é como se estivesse sendo publicado na capa de um grande jornal de circulação nacional. A partir do momento que se publicou ali, você não tem mais controle sobre aquele conteúdo, aquele conteúdo pode ter sido replicado e você não tem mais controle, tá? E denuncie. Você viu algo suspeito? Denuncie. Nós precisamos ter a Internet para o uso e a facilidade, a produtividade que deu na economia como um todo. Esse é o objetivo da Internet, essa é a parte fantástica de ter uma rede mundial. Ela pega em qualquer lugar do mundo com diversas formas de conexão e permite lazer, ela permite educação, permite trabalhar, está permitindo que nós façamos esta live. Isso tudo está baseado dentro da Internet. Então, ter esta rede de uma forma segura o suficiente para que todos possam aproveitá-la é um grande objetivo que a gente tem que colocar, e no caso das teles a gente tem feito... tem dado uma importância muito grande para toda essa parte de educação e de bom uso, o bom uso e uso responsável dessa rede.

Obrigado a todos.

SR. ANTONIO MARCOS MOREIRAS: Muito obrigado, Paulo. Então, gente, agora, a gente já teve os representantes aí das grandes empresas de telecom, das empresas de telecom, e dos provedores e dos pequenos prestadores de telecom falando. Vamos ver agora os outros setores.

E o próximo setor, agora, é de fabricantes de equipamentos, os *venders*, representados aqui pela Cisco, pelo Fernando Zamai. Então, Fernando, muito obrigado por ter aceito o convite de estar aqui com a gente, e o palco é seu. Por favor, faça a sua apresentação.

SR. FERNANDO ZAMAI: Bom dia. Bom dia, Antonio. Bom dia a todos. Eu que agradeço o convite. Acho que é uma honra poder aqui falar de um assunto que eu gosto muito e passar um pouco da visão de quem desenvolve soluções e quem fornece no mercado. Eu não vou colocar uma apresentação em si... Desculpa que a minha voz está um pouco ruim, estou passando aí por uma crise de resfriado, não é, essa mudança de tempo aí que vem afetando, principalmente em São Paulo. Eu estruturei a minha apresentação tentando aqui colocar e mostrar tudo o que a gente vem fazendo como fabricante para impulsionar o tema ciber, que hoje permeia desde CPF, pessoa física, até pessoa jurídica, e a gente atua muito com as empresas também, não é, e separar em tecnologia, processos e pessoas, onde que a gente atua em cada uma dessas áreas. E eu acho que o tema maior, ele foca em cima de quanto que se investe em segurança, e não só investimento financeiro, mas investimento de tempo, não é, o quanto se dedica. Então, essa live que a gente está fazendo hoje aqui já é uma mostra desse investimento, uma preocupação, não é? Então, não vou me

apegar nas N notícias que vêm acontecendo, acho que tudo isso vem puxado pela transformação digital, então todo mundo conectado, todo mundo com supercomputador na mão, que são os celulares, os dados, não é, a vida das empresas, das pessoas, hoje totalmente virtual, armazenada em uma nuvem, em um celular, [ininteligível], toda essa transformação, essa nova realidade que a gente vive, trouxe cibersegurança como um tema extremamente relevante à tona, e essa relevância vem de um questionamento de quanto cada um de nós investimos nisso, não é? E olhando para as empresas, onde que cibersegurança é debatido, se é debatido no executivo ou na área técnica. Hoje, as empresas mais maduras debatem o tema no corpo executivo. Na área militar, os Estados Unidos colocaram como quinto domínio de defesa: ar, mar, terra, espaço, *cybersecurity*. O que significa isso? Significa uma estrutura inteira com investimento no tema ciber para tratar o *cyberwar*. Pessoa física seria uma reflexão de quanto tempo cada um de vocês investiu para ativar o segundo fator em todas as suas contas, as suas mídias sociais, não é? Então, para fazer exatamente aí o que o meu colega citou, trocar senha, senha segura, administrar senha, que é difícil, e é chato ficar administrando. Eu vou falar depois o que a gente está fazendo no setor de tecnologia para simplificar isso, mas o quanto que cada um de nós investiu de tempo para nos proteger, fazer uma higienização aí de ciber, não é, e também para orientar a nossa família. Eu acho que é uma missão de nós, que conhecemos a tecnologia, conhecemos como funciona a Internet e seus riscos, levar isso para dentro de casa. Então, fazer... eu já fiz treinamentos com os meus filhos, com a minha família, com a minha mãe... Minha mãe me liga, não é? Ela recebe lá um documento, alguma coisa anexada, ela já me liga e pergunta se pode clicar. Agora, se ligou, já nem clica, não é? Então, se está preocupada, já nem clica. Então, essa conscientização é um conjunto de ações que a gente vem investindo no Brasil.

Começando por pessoas. A gente tem uma academia, que é a Cisco Networking Academy, e essa academia, agora, ela se estruturou para oferecer cursos de tecnologia em ciber, que é o cibereducação, é o programa CiberEducação. Então, a gente montou um programa gratuito em parceria com o Sesi, com o Centro Paula Souza, onde estamos formando profissionais para o mercado em ciber. E isso... depois a gente estabelece uma conexão com as empresas para que as empresas consumam esses profissionais, não é, que já saíam ali com uma formação. Por quê? Tratando a carência de expertise em cima do tema, fizemos um investimento muito grande no Brasil para montar um centro de inovação na Distrito Fintech, na Rebouças, ali em São Paulo, no bairro de Pinheiros, onde é um centro para acontecer esses debates, não é? Então, até eu espero quando acabar, todo mundo vacinado, não é, acabou essa crise que a gente vive aí da pandemia, a gente possa fazer essa próxima live desse CyberHub, que é um centro para fomento da discussão cibercomunidade e investimento em

startups, startups brasileiras que estão aí começando a crescer em torno do assunto de ciber.

Falando em tecnologia... Então, aqui eu acho que eu peguei os dois principais pontos ali em cima de pessoas. Falando em tecnologia, os produtos, eles já possuem um arsenal de recursos para proteção. Existe um arsenal de recursos que saem dos produtos, e esses recursos, eles têm um custo associado. Existe um preço que eu pago por ele. Então, existe um preço por tempo de ativação, existe um preço para consumo de tecnologia. Vou dar um exemplo de uma das tecnologias que é extremamente crítico. A gente tem um centro de inteligência, Talos, de cibersegurança, e em 2018 foi diagnosticado aí um grande ataque massivo contra CPEs, contra equipamentos que sustentam aí as conexões da Internet, chamado de VPNFilter. Esse ataque constituía onde os atores que, enfim, fizeram o ataque trocaram o código do produto. Então, era uma linha de produtos de baixo custo, produtos mais baratos, e aí vai de encontro ao início do investimento, e os atores, eles trocaram o código e colocaram código deles naquele produto, e o código deles poderia fazer desde *sniffing*, desde captura de pacotes, eles poderiam fazer o que quiser com aquele dispositivo, inclusive lançar grandes DDoS, não é? Ou seja, eles dominavam o CPE, o equipamento que está dentro da casa das pessoas, dentro da empresa. A partir da... Lá atrás, puxando mais para atrás, o que a gente fez sobre esse tema? Todos os produtos saem hoje assinados, não é, então saem com um chip de criptografia dentro do produto para fazer algo chamado como *Secure Boot*, não é? O hardware, quando inicia, ele valida se o certificado veio do desenvolvedor, do fabricante, para garantir que o código que está rodando naquele dispositivo é do fabricante que detém aquela tecnologia, para inibir que alguém possa fazer a troca desse código. Isso tem um preço, não é? Esse chip que vai adicional nos equipamentos, ele vai custar um pouquinho mais caro do que os equipamentos que não têm aquilo ali. Então, volta ali no tema também de quanto se investe em cibersegurança hoje de maneira geral, e é um processo ou uma transição.

Falando em cima do produto ainda, um programa muito sério administrado é chamado *Product Security Incident Response Team*. Todas as vulnerabilidades encontradas nos nossos produtos são levadas muito a sério, existe um processo, tecnologia, processo e pessoas, existe um processo que se você que está nos assistindo agora encontrou uma vulnerabilidade e entende que é crítica e fizer o *report*, vai ser tratado com prioridade, com atenção, de acordo com a severidade, e será publica a correção, e várias vezes já aconteceu de o produto ser removido do mercado. Dependendo da severidade, esse time, ele tem autonomia para remover o produto do mercado, chamar os desenvolvedores e falar assim: "Esse produto só volta na hora que for corrigido". Então, assim, tratar com seriedade que existem vulnerabilidades, não é, e existem em todos os produtos, é muito

importante, tratar o tema com consciência, tratar com maturidade para assumir que não existe solução infalível, erro humano, erro no código, muita biblioteca, não é, que foi importada, que já vem lá com alguma vulnerabilidade, tratar esse tema é muito importante. Segundo ponto: falei de *Secure Boot* para o... o *Product Security Incident Response Team*, conscientização para ativar os recursos, não é? Então, assim, quanto tempo você vai investir para ativar? Porque ativar você pode tirar uma conexão do hardware, vai demorar um pouquinho mais, eu tenho que treinar a equipe que vai ativar aquela segurança, não é? Então, tudo isso se casa, e vem acontecendo aí gradativamente.

E do ponto de vista de desenvolvimento, estamos trabalhando na simplificação. Eu acho que o melhor exemplo de simplificação de segurança e tecnologia avançada seriam os próprios smartphones, não é? Então, hoje, a gente consome autenticação por reconhecimento facial, biometria, diversos recursos que o smartphone nos coloca à disposição já ativados e uma tecnologia extremamente avançada para nos proteger. Então, a gente vem trabalhando nessa simplificação, em como que eu ativo a segurança, porque aí se junta com uma outra iniciativa, chamada *Software-Defined Networking*, que [ininteligível] toda essa iniciativa do *Software-Defined* veio para simplificar como eu ativo as configurações de um roteador, de um switch, de um firewall, como que eu simplifico, como que eu integro, como que eu unifico, para tornar mais simples o consumo daquilo que é mais complexo, tá? Então, um exemplo disso seria a linha de produtos Meinecke totalmente na nuvem, ativa, a VPN, você dá um clique, ativa. A VPN Cisco, no passado, você tinha que ter um livro de 5 mil páginas para ativar uma VPN, não é? Então, essa simplificação, ela já vem acontecendo, já está disponível em todas as linhas.

Falando em processos, eu citei que a gente tem uma central de inteligência, Talos. Talos administra alguns programas: é um programa de troca de informação com empresas chamadas *edges*(F) onde a gente troca inteligência ciber, quais são os ataques que estão acontecendo, as características, as preocupações, as novas táticas, as novas técnicas; programa Crete, onde a gente coloca sensores dentro das empresas, dentro do *service provider*, para monitorar o tráfego e entender o que está acontecendo; e, ao mesmo tempo, a gente administra comunidades, a comunidade do Snort, comunidade do Clam Antivirus, onde a gente publica para o cidadão em formato de software livre, onde você pode consumir alta tecnologia através disso. E uma mudança de conceito, que é o *zero trust*: confiar menos, não é? Todos nós devemos confiar menos nas conexões, no SMS que chega pelo telefone. Então, assim, ter um critério de segurança mais... ter níveis de concessão de confiança com critérios mais elaborados, não é? Nós, como ser humanos, o brasileiro, principalmente, nós confiamos muito. Então, essa mudança de mentalidade afeta redes, afeta vidas, afeta tudo isso. E por fim, o desenvolvimento da tecnologia onde a senha...

estamos trabalhando para não ter mais senha. A entrada nos sistemas, a entrada nas soluções ser 100% orientada em cima de reconhecimento facial, com *back-end* integrado, onde eu faça de forma segura e garanta o acesso, tá?

Então, esse era o meu *pitch* ali para colocar um pano de fundo do que é que do lado do fabricante, o que a gente vem fazendo aí para tornar a nossa vida mais segura, e eu vejo uma evolução muito grande, não é? Marco Civil da Internet, Lei Geral de Proteção de Dados, tudo isso é benefício, tudo isso coloca a ciber na pauta, e, gradativamente, a gente vai melhorando as proteções e tornando aí a Internet mais segura.

SR. EDUARDO BARASAL MORALES: Tá certo, Fernando. Muito obrigado pela sua apresentação, foi muito interessante.

Bom, agora, eu gostaria de continuar chamando a Vanessa Copetti Cravo, da Anatel. Vanessa, fica à vontade.

SRA. VANESSA COPETTI CRAVO: Obrigada, Eduardo. Um bom dia a todos e todas que estão nos assistindo. Gostaria também de cumprimentar os painelistas e agradecer ao NIC, ao NIC.br primeiro pela iniciativa e de colocar esse tema tão relevante em pauta, e, segundo, o convite à Anatel, uma excelente oportunidade de a gente apresentar o que a Anatel está fazendo em matéria de segurança e também os esforços de todos os setores de telecomunicações. Eu vou compartilhar uma pequena apresentação com vocês. Um segundo. Acredito agora que vocês já estão visualizando a apresentação.

Bom, para falar de segurança na Internet, a gente tem que retroceder aqui um degrau e falar também de segurança de telecomunicações, falar de segurança do setor que vai prover justamente... vai possibilitar a conexão à Internet. Nesse sentido, a segurança das redes para a Anatel é vista como um tema prioritário, um tema transversal, que é horizontal e transpassa todos os setores da economia, todas as atividades da sociedade, todos os órgãos e entidades da administração pública federal e também internamente, na agência, não é? Várias áreas da agência internamente tratam desse tema. Ele também é um tema multidisciplinar, porque ele aborda, envolve várias áreas do conhecimento, e, finalmente, ele é um tema multissetorial. Nós temos uma responsabilidade compartilhada em que cada um dos atores de toda essa cadeia tem um papel a ser executado.

Nesse sentido, como a Anatel está atuando? A Anatel há muitos anos, ela vem atuando na promoção de segurança e resiliência das redes de telecomunicações, e, basicamente, ela tem três frentes: uma frente relacionada à regulamentação, uma frente direcionada à conformidade e homologação dos equipamentos que são interconectados e para possibilitar essa conexão à Internet e, finalmente, e não menos importante, e dialoga muito com os outros

painelistas, com as falas que me antecederam, é justamente uma vertente relacionada à conscientização.

Bom, no tocante à questão da regulamentação, a Anatel, no final de 2020, ela editou um regulamento específico de segurança cibernética aplicado ao setor de telecomunicações, e, basicamente, ele pode ser compreendido em seis blocos: um bloco das disposições gerais iniciais, que vai tratar todas as definições do regulamento, inclusive abrangência; um bloco que trata de princípios e diretrizes que são aplicados a todas as prestadoras de telecomunicações; um bloco direcionado às obrigações que são mandatárias para todas as prestadoras que não são de pequeno porte; finalmente um bloco que vai tratar, então, de como a Anatel vai atuar nessa maneira; ainda um bloco relacionado à questão das sanções, lembrando que a Anatel já, agora, criou um novo paradigma sobre essa ótica da regulação responsiva e quando ao comportamento dos regulados; e, finalmente, as disposições finais, que trazem os prazos de adaptação ao regulamento.

Bom, e quais as obrigações que as prestadoras têm que atender? Na época da fase de regulamentação, é elaborada uma Análise de Impacto Regulatório, onde se detecta alguns problemas, alguns pontos de atenção para o regulador, e que justamente, motivam então a edição de uma regulamentação, não é? Um dos problemas elencados foi justamente a necessidade de governança pelas prestadoras desse tema, e uma governança no mais alto nível estratégico das empresas, que dialoga muito com o que foi falado anteriormente também. Isso tem que ser uma prioridade. E isso, então, ele é resolvido com a edição de uma Política de Segurança Cibernética e que também tem que ser conhecida pelos usuários daquela prestadora. E ela vai ser conhecida a partir, então, da publicação desse extrato, do que é possível, do que não é sensível, no site da prestadora. Além disso, foi identificado como uma necessidade que a Anatel passe a ter um diagnóstico dos incidentes no setor, e, para isso, as prestadoras precisam notificar a Anatel. Além disso, também é necessário que as prestadoras compartilhem informação entre si, porque o ataque de uma prestadora hoje é o ataque de amanhã em outra, e, também, um incentivo especial para que as prestadoras de pequeno porte possam também ter acesso a essas informações, porque também foi detectado que, obviamente, elas têm menos acesso a essa parte de inteligência. Além disso, já um olhar com relação aos fornecedores, não é, a cadeia de fornecedores, e por isso as prestadoras... os fornecedores das prestadoras também precisam ter uma política de segurança cibernética e também sofrer processos de auditoria. Além disso, um olhar aos equipamentos que são cedidos aos usuários, especificamente na questão da configuração e autenticação deles, um olhar também bastante importante relacionado ao tratamento de vulnerabilidades, que também foi mencionado na fala do Fernando, e por isso as

prestadoras precisam executar ciclos de avaliação de vulnerabilidades, e, finalmente, enviar informações sobre as infraestruturas críticas à Anatel.

Além disso, o regulamento, ele também busca resolver o problema da governança de segurança cibernética no setor, e ele faz isso através da criação do Grupo Técnico de Segurança Cibernética e Gestão de Riscos de Infraestruturas Críticas, o GT-Ciber. Ele nasce com um rol bastante extenso de atribuições justamente para se tornar o *locus* de segurança cibernética de todas essas discussões no setor. E entre as atribuições, eu posso citar: auxiliar o acompanhamento da Política de Segurança Cibernética pelas prestadoras, dispor sobre a forma e procedimento de atendimento dessas obrigações, acompanhar o procedimento de compartilhamento de informações, propor internalização de boas práticas e padrões, incentivar ações de capacitação, propor ações de conscientização e elaborar estudos.

Além disso, o GT-Ciber, ele nasce com uma estrutura, de certa forma, executiva, que a gente denomina de plenária, que é composto pela Anatel, prestadoras de mercado significativo e também uma representação das prestadoras de pequeno porte, e ele conta com um terço dos grupos técnicos, um destinado à Política de Segurança Cibernética e Gestão de Infraestruturas Críticas, um grupo destinado ao compartilhamento de informações e boas práticas, não é, e uma das boas práticas que a gente vem discutindo já há algum tempo é justamente o MANRS, que foi abordado pelo Parajo, na fala dele, no início, e esse grupo também conta com a presença... com a forte presença que vem aportando expertises sempre do Cert.br, e também um subgrupo técnico de equipamentos, fornecedores e requisitos, que vai focar todo esse olhar para essas outras obrigações.

Com relação ao segundo pilar, que foca especificamente na questão de tecnologia dos equipamentos, logo após a edição do regulamento de segurança cibernética, também foi expedido o Ato 77/2021 da Superintendência de Outorga e Recursos à Prestação, e ele, justamente, ele aprova requisitos de segurança cibernética para os equipamentos, trazendo as recomendações aos fabricantes e fornecedores de produtos e também estabelecem o programa de supervisão de mercado. Quando a Anatel vai, ou por ofício, por iniciativa própria, vai avaliar vulnerabilidades em equipamentos, ou vai agir após uma denúncia, e, eventualmente, pode, se o fornecedor não resolver não sanar as vulnerabilidades encontradas no prazo estabelecido pela Anatel, pode ocasionar suspensão da homologação daquele produto e, eventualmente, até mesmo a retirada do mercado de consumo de todos esses equipamentos.

Finalmente, não menos importante, que dialoga também com todas essas falas, não é, o foco em conscientização, e nisso nós temos o movimento Fica Esperto, que eu imagino que muitos de vocês devem

ter recebido um e-mail, um contato da sua prestadora, ou até mesmo um SMS relacionado a esse movimento, e ele nasce no âmbito de uma fiscalização regulatória da agência como uma demanda para as prestadoras do setor e acaba expandindo, envolvendo a comunidade técnica, até mesmo o NIC.br, e, finalmente, inclusive, ultrapassa esse setor telecom e Internet para envolver também o setor financeiro. E além disso, uma outra vertente no site da Anatel, anatel.gov.br, não é, vocês têm uma página dedicada para a segurança cibernética, que ali contextualiza toda a ação da Anatel, trazendo todos os marcos normativos, Política Nacional de Segurança da Informação, Estratégia Nacional de Segurança Cibernética e, finalmente, mais informações então sobre o regulamento, sobre o ato, os links associados e também pelo GT-Ciber.

Eu agradeço essa oportunidade mais uma vez ao NIC.br, e agradeço, e estou à disposição para perguntas. Obrigada.

SR. ANTONIO MARCOS MOREIRAS: Nós é que agradecemos, Vanessa. Eu aproveito para perguntar novamente para o pessoal que está acompanhando a live aí ao vivo no Youtube e nas outras plataformas, no Facebook, no LinkedIn, como é que está a transmissão, se normalizou, como é que está agora a imagem, para a gente ter uma ideia aí, para vocês darem... deem um feedback para a gente de como estão as coisas. E aproveito para pedir, gente, a gente tem 540 pessoas acompanhando agora ao vivo, deem o *like*, deixem o seu *like* na live, porque isso ajuda o Youtube a fazer a distribuição orgânica e acaba... mais gente acaba tendo acesso a esse conteúdo, seja agora, ao vivo, seja depois, no conteúdo que ficar gravado. Que bom saber que para... a maior parte das pessoas que está dando feedback está dizendo que a transmissão está boa, que o áudio está bom também. Então, está dando para vocês acompanharem, porque o conteúdo realmente está bastante interessante e é superimportante.

Eu vou chamar agora o Alê Borba, do Google, para fazer a sua apresentação inicial. Alê, por favor, o palco é seu.

SR. ALÊ BORBA: Olá, olá. Obrigado, Moreiras. Bom, primeiro, bom dia aí a todos. Obrigado pelo convite e por todo mundo estar participando aí hoje. Bom, como já falado, sou Alê, Alê Borba, eu trabalho no Google, na parte de *Trust & Safety*, uma parte que cuida de segurança, principalmente de usuários e políticas de uso. E, bom, falando um pouco aqui sobre essa parte de segurança e papel de cada um, eu gostaria de começar falando que não é de interesse de nenhuma plataforma de conteúdo que as suas plataformas sejam usadas de forma a enganar as pessoas, ou seja abusado de qualquer forma, tá? E aí, nessa área, eu costumo falar com todo mundo que a gente não existe... não existem competidores, só existem parceiros, porque é de interesse de todo mundo que isso não aconteça nas plataformas, tá? Então, eu queria só começar com esse ponto.

E eu acho que todo mundo colocou muito bem aqui, o Parajo colocou isso no começo também, que é muito bacana essa parte de não importa... Todo mundo tem que participar. Eu acho que o Paulo falou isso bem, e todo mundo tem que engajar no uso ético e correto da Internet, isso é muito importante. Então, é papel não só dos provedores de conteúdo, das plataformas, dos fabricantes, mas... e também dos usuários. Eu acho que é para todo mundo isso. Então, hoje, se você tem aí todos os seus hardwares muito bem protegidos, muito bem configurados, os sistemas muito bem protegidos, as plataformas com proteções e tudo, mas o usuário também não colabora muito, não faz parte dessa equação, isso se torna um problema, não é? O Paulo bem colocou junto com o Parajo... Por exemplo, uma máquina comprometida, uma máquina desatualizada, o Parajo colocou o Paulo123... o Parajo não, o Paulo colocou lá a senha Paulo123, uma senha muito fraca, e isso pode comprometer a segurança do usuário, isso também compromete a segurança do usuário.

Então, hoje, uma coisa que todo mundo tem feito muito, e aí aqui ficou claro também que todas as áreas também têm feito isso, é um trabalho de educação digital, de consciência digital, muito grande. Hoje, a gente tem... e aí, citando especificamente o Google, a gente tem um projeto muito bacana, que chama Seja Incrível na Internet, e ele é bem focado em pais e professores. Por quê? Porque a gente acredita que a gente tem que educar todo mundo, mas educar também essas pessoas, as crianças e adolescentes que estão chegando agora, é muito importante. Por quê? E através dos pais, não é? Por que isso? Porque o que eu muito escuto hoje em dia é: "Ah, não...", um pai de um adolescente, por exemplo, "ah, não, o meu filho sabe tudo de Internet. Então, eu não entendo nada". E isso não é bem verdade, não é, gente, a gente sabe disso. Assim, eles sabem... as crianças e adolescentes hoje, eles têm uma facilidade de usar a tecnologia, mas eles não têm esse conhecimento todo do que é certo, o que é errado. Então, os pais têm que ficar muito próximos e ajudar. Então, a gente tem esse trabalho de conscientização por que? Porque eles são o futuro da Internet, tá? Então, você saber o que está compartilhando, você usar uma senha forte... Então, a gente tem esse trabalho de conscientização muito grande hoje em dia e, junto disso, a gente trabalha com vários... a gente tem várias coisas hoje para evitar que esse tipo de conteúdo também se espalhe, um tipo de golpe, alguma coisa, se espalhe nas nossas plataformas. Então, por exemplo, falando um pouco aí de um dos últimos relatórios de transparência que a gente publicou, só em 2019, se não me engano, foram removidos 36 milhões de anúncios fraudulentos, sabe? Então, assim, é um número grande, e são remoções proativas.

Outra coisa que as plataformas também têm facilitado cada vez mais, e eu achei muito bom isso que o Fernando também colocou, que

é a simplificação dos processos. Então, hoje, a gente tem tentado cada vez mais deixar mais fácil para os usuários reportarem alguma coisa de mal que estão ali vendo, entendeu? Porque por mais que a gente tenha várias tecnologias ali, tal, da mesma forma que as tecnologias, elas evoluem, infelizmente, os maus atores, eles também evoluem, e eles evoluem muito rápido. Então, nessa área de tecnologia... de segurança a gente costuma brincar que é aquela corrida de gato e rato, não é? A gente está... vai, e eles melhoram, a gente vai atrás de novo e eles melhoram. Então, a gente sempre deixa e tenta simplificar ainda mais esses processos de *report* do usuário. Então, o usuário foi lá, ele viu alguma coisa que ele percebeu, que ele viu que não é algo que deveria estar ali, ele tem um botão para reportar isso para a gente, e isso é analisado e removido. De novo, não estou falando isso também só como Google. Estou aqui representando o Google, também os [ininteligível] de conteúdo, mas estou falando de toda a indústria de conteúdo, hoje, você tem uma forma, e essa forma está cada vez ficando mais fácil de se fazer. Por quê? De novo, a gente tem que realmente simplificar os processos, não é? Então, outra coisa também que a gente tem trabalhado muito ultimamente é essa parte de senha. Além da educação, hoje a gente tem um *check-up*. Você pode entrar na sua conta do Google e fazer um *check-up* de segurança da sua conta. Você entra lá e tem todos os tiquezinhos para ver se você tem uma senha forte, verificar se sua senha é forte, verificar se a sua senha apareceu em algum vazamento de dado. Então, tem todas essas checagens de segurança, e também checagem de privacidade, porque a ideia aqui não é dificultar, a ideia aqui é justamente facilitar, simplificar esses processos para tornar... Porque assim, se você faz... você cria um processo de segurança difícil para o usuário, isso acaba sendo uma barreira, não é? Então, tem todo esse trabalho do nosso lado.

Uma outra coisa também que a gente tem feito muito na área um pouco mais técnica é, de alguma forma, compartilhar com a indústria, com outros *players* do mercado, as tecnologias que a gente tem. Então, hoje, por exemplo, a gente tem duas tecnologias hoje que são para combate de... são abusos específicos, um tipo de segurança específico para combate a abuso infantil. A gente tem um site para isso, na verdade, está até também traduzindo em português, apesar de o link em inglês, não é, protectingchildren.google. Então, esse site, você abre, ele está em português, e lá nós temos duas APIs que a gente compartilha com a indústria para ajudar a indústria a melhor combater, identificar e remover rápido, ou nem deixar que isso suba para a plataforma, conteúdos de abuso infantil, que é uma... chama Content Safety API, e o CSI *match*, com a tecnologia que a gente usa no Youtube, que a gente também disponibiliza para a indústria. Então, como eu disse no começo, a gente não tem aqui... E tudo gratuito, tá, gente? A gente não tem aqui concorrente, tá, a gente tem vários parceiros nessa área, inclusive, nessas duas ferramentas, a gente tem

outros *players* grandes da indústria que também usam. A SaferNet Brasil é uma ONG brasileira que usa essas ferramentas, é uma outra forma também de parceria que a gente tem hoje, além aí de outros *players*. Assim, a gente não tem só essa ferramenta que a gente compartilha com a SaferNet, a gente tem outros... tem treinamentos que a gente faz com eles, mas justamente, assim, para sempre... visando a simplificação de processos, a remoção rápida desse tipo de conteúdo das plataformas e também apoiando essa educação digital, porque para nós, realmente, a educação digital, ela é importante, ela é muito importante, porque se o usuário, ele... o nosso... a pessoa ali que está usando ali as plataformas, eles usam de uma forma consciente, com todas as habilitações de segurança e tudo, isso só ajuda mais ainda que isso tudo fique... o ecossistema inteiro fique mais seguro e evita que isso aconteça. E aí, só para finalizar aqui nessa parte de criança, que eu acho que vale citar também, a gente tem hoje várias coisas específicas para esse público, inclusive, que a gente pensa ser hoje um dos mais vulneráveis também, que são as crianças e os adolescentes, e, hoje, muitos pais não sabem o que fazer e tudo o mais. Então, hoje, tem algumas ferramentas... Então, por exemplo, a gente sabe que a idade, hoje, média para uma criança que tem o seu primeiro telefone, dela mesmo, está na faixa de dez anos. A gente tem um recorte, é claro, de local e tudo, mas no geral, no Brasil, dez anos, tá? Então, a gente tem hoje o Family Link, por exemplo, que é um aplicativo que você pode... que os pais podem instalar, e eles controlam totalmente essa conta, esse celular, ou o que o filho está fazendo, assim, com quem está conversando e tal, que também é uma forma de ajudar nessa segurança das crianças e ajudar nessa parte de educação também.

E aí, eu vou parar por aqui, para a gente começar essa discussão, e a gente fica aí disponível para as perguntas. Obrigado aí de novo pelo convite e pela iniciativa aí do NIC.

SR. EDUARDO BARASAL MORALES: Muito obrigado aí, Alê Borba. Realmente foi muito interessante tudo o que você colocou.

E, para a gente finalizar nessa rodada de palestrantes, eu gostaria de chamar a Cristine Hoepers, que é aqui da casa, para falar um pouquinho do nosso papel nessa questão de segurança. Então, Cristine, fique à vontade.

SRA. CRISTINE HOEPERS: Obrigada, Eduardo. É muito bom participar de novo dessas lives aí, a gente está sempre compartilhando informações e tentando entender melhor aí como que cada um pode fazer o seu papel na segurança, não é? E até... [ininteligível] para mim falar um pouco aí de comunidade técnica, não é? É engraçado que é um termo que a gente usa muito, mas assim, quem é a comunidade técnica? No fundo, é todo mundo também, porque nas teles tem comunidade técnica, nos provedores tem, na área de conteúdo, mas a

gente lembrar que, em geral, a gente tende nessa área técnica de Internet a não pensar muito em outras camadas, ou ter uma visão muito focada ali de como que eu faço isso funcionar e não necessariamente como é que eu faço ser seguro, não é?

E uma coisa que eu queria refletir, não é, como eu estava falando por último, eu falei: Ah, deixa eu tentar dar uma costurada, não é, acho que em tudo o que a gente está falando de todas as áreas aí. Porque quando a gente fala em segurança, o Fernando lá, ele comentou: "Ah, a gente tem hoje isso na agenda de defesa", não é? Sim, a gente tem hoje aqui no Brasil, a gente tem o Comando de Defesa Cibernética, nos Estados Unidos tem o Cyber Command, você tem muitos lugares onde você tem o pessoal de defesa cibernética, mas, nessa pirâmide, por que eu coloquei eles em cima? Porque, no fundo, aqui não é uma pirâmide de priorização ou de hierarquia, eu estou querendo mostrar um pouco como é que aumenta a complexidade técnica, você sai um pouco do nível mais político de diretrizes, e como é que aumenta a dependência do nível anterior quando a gente pensa em segurança e quando a gente começa a pensar em coisas técnicas, porque se a gente pensa em defesa cibernética, o pessoal no chat do Youtube falou muito ali: "Ah, mas e os russos?", "e como segurar os ataques?", está todo mundo está falando de ransomware, tal. Sim, mas não tem como a gente botar tropas na rua para proteger o computador que está dentro das empresas, dentro da nossa casa. Eu acho que a gente tem que pensar que quanto mais a gente está falando em defesa, em estratégias de segurança cibernética que hoje já tem, não é, a gente tem... a Vanessa apresentou bem como são todas as estratégias do setor de telecom, a gente tem o GSI definindo estratégias para o governo como um todo, a gente tem o Comando de Defesa Cibernética fazendo os exercícios de defesa, mas, no fundo, o que é tudo isso? É uma maneira de você dar um norte, de você dar uma certa direção para o que precisa ser feito do ponto aqui de segurança e administração de sistemas e o que tem que ser feito para resolver quando tiver um incidente. Mas mesmo essa segunda camada de baixo para cima aqui, que já é mais técnica em natureza e que é aqui que a gente está falando em aplicar ferramentas de segurança, os equipamentos, e pensando em como agir quando tem um incidente de segurança, tinha muita gente também no chat falando de LGPD e de proteção de dados, quer dizer, a gente está aqui... isso tudo também não vai resolver o problema, quer dizer, não adianta a gente dizer: "Eu tenho firewall", "eu tenho antivírus", ou "eu criei uma política", se tudo isso está em cima de uma base que é uma base que não é sólida, não é? E o que é essa base? É onde a gente tem o mais técnico da comunidade técnica, é onde a gente tem o pessoal pensando em projeto de protocolos, não é? A gente está pensando aqui em desenvolvimento de sistemas e aplicações. Então, esse é um ponto em que quem está lá projetando como vai ser a próxima versão do DNS, como é que a gente vai usar DNSSEC, o pessoal fazendo

protocolos que não estão em IETF, não é, muita gente reclamando: "Ah, mas o protocolo SS7", "o GSM', tal... Pessoal, isso tudo é discutido em órgãos que estão definindo protocolo. Se o projeto não prevê a segurança, não tem muito o que a gente consiga fazer depois, não é? A gente pode daí pensar em colocar ferramentas, em monitorar, em fazer gestão de incidentes, em reduzir o número de problemas, mas tem problemas que são inerentes dos sistemas, e eu acho que aqui é o ponto onde a gente tem que engajar todos da comunidade técnica, que até nem estão aqui nessa live, porque eles não são os provedores, não são as Telcos, não são uma empresa de conteúdo, mas é o pessoal que está desenvolvendo tudo o que a gente usa. E eu acho que isso é uma coisa que a gente precisa ter consciência, que, hoje, quase tudo é software, e tudo está conectado na Internet. Os ataques, eles têm motivações múltiplas, a gente acaba vendo muito a motivação financeira, a motivação de estado, de ataques entre nações, que agora não sai da mídia, mas a gente precisa pensar que tudo isso está rodando em cima de software, em cima de protocolos que são discutidos em fóruns técnicos e a gente precisa ter essa base segura para a gente poder aí, sim, colocar mais segurança em cima, porque as áreas de segurança das organizações não são mágicas, elas não vão conseguir resolver todos os problemas, e incidentes vão acontecer, porque são seres humanos que estão fazendo a tecnologia, que estão implantando. As tecnologias não são perfeitas, a gente precisa estar preparado para lidar com isso. Eu acho que esse é um ponto que a gente tem que levar muito em conta.

E pensar... quando eu falo aqui dos ataques, pessoal, a gente precisa cuidar do básico primeiro, não é? Muita gente falou: "Nossa, mas os russos...". Olha, infelizmente, eles não estão usando tecnologia espacial para invadir o governo americano, não é? A gente olha hoje, até essa semana saiu mais um relatório bem detalhado, pessoal, é muito deprimente. Já estou falando aqui o que é reportado para o CERTt.br. O que a gente mais vê é uso de senha fraca e serviços que só têm senha, que são expostos, como vazamento, força bruta, e a quantidade de desenvolvedores que sobem sistemas no GitHub *pastebin* com as senhas e com as chaves de autenticação é absurda, tá? Todo aquele ataque dos russos no governo americano, que foi aquele SolarWinds saiu esse ano, tudo começou com uma senha que foi subida no GitHub do fabricante da SolarWinds. Eles subiram um software no GitHub que expôs a senha do servidor FTP, onde ficavam os *patches* do sistema. E aí, o pessoal viu que essa senha foi exposta, pegou essa senha, conseguiu alterar *patches*, alterar apelido de segurança, que daí alterou o sistema do fabricante, que aí alterou os softwares no fabricante. Então, quer dizer, pensar que tudo começou com uma senha, não é? Esse ano também foi aquela questão do Colonial Pipeline, que saiu do ar todo o suprimento de combustíveis lá da costa leste americana. Senha, uma senha de VPN que foi vazada na *dark web*. Então, assim, pessoal, a gente tem que pensar que são

coisas que... "Ah, mas foi um descuido". Sim, mas é com esses descuidos que está começando, é com a falta de aplicação de *patches*, não é?

Outra questão que tem comprometido muito redes de governo é falta de aplicação de *patches*, que já existem há três, quatro, cinco anos, mais às vezes. Eu até deixei um link no Youtube de uma palestra onde a gente vê muitos detalhes. E eu acho que aí uma função da comunidade técnica não é ficar esperando que venha uma lei que vai proteger ou ficar esperando que eu vou ter alguém me dizendo para fazer ou mandando, mas é todo mundo tem que fazer a sua parte, seja usuário final, seja administrador da operadora de telecom, seja alguém de outra organização. Quer dizer, precisa aplicar *patches*, precisa ter segundo fator em todas contas, pessoal, e tem que cuidar de erros humanos, porque a gente vai cometer erros, tem que ter mais atenção, não é?

E eu acho que... assim, eu vi uma palestra muito interessante da Katie Moussouris esse ano, ela, que mantém aí... foi a primeira pessoa a pensar em *bug bounty*, instituir os programas de *bug bounty* da Microsoft, ela deu um *up* em toda essa parte de aplicar *patches*, e ela tinha... Um conselho para as empresas era: "Ponha múltiplos fatores em tudo", não é? Então, pensem que essas são decisões gerenciais e técnicas, mas a comunidade técnica é que tem acho que o poder de colocar.

Pessoal, e assim, para não deixar esse slide de fora das minhas palestras, pessoal, assim, estamos em 2021, já passou da hora de adotar protocolos mais modernos, já passou da hora de a gente ter IPv6 no conteúdo e nos provedores, já passou da hora de começar a pensar em RPKI e segurança de roteamento, o Parajo falou muito de MANRS, falou de tudo isso, vocês sabem como a gente está fazendo essa evangelização. Quem tem servidores de e-mail, se você é um banco, se você é um órgão de governo, se você tem qualquer site de conteúdo que tenha e-mail, ponha DNSSEC, ponha STARTTLS, DMARC, DKIM, ajude o Google a filtrar os spams em nome da sua organização que chegam na conta dele, ajude todos os provedores a conseguir filtrar fraude nos e-mails, não é, usem DNSSEC para a gente conseguir ter outras tecnologias em cima, poder ter DANE, poder ter segurança maior. A HTTPS, TLS, *forward secrecy*, HSTS, pessoal, coloquem cripto em tudo. Não faz mais sentido, não tem *overhead*, não pensem nesse mito de que é pesado para rodar. Ponha um segundo fator, seja em hardware, seja em software, usem isso, não é? A gente pôs aqui os protocolos do IETF. Vocês podem usar o autenticador da Microsoft, o Google Authenticator, ou podem fazer o autenticador de vocês. O protocolo é aberto, padrão e aberto, não é? Usem isso de qualquer maneira.

E o pessoal que não está muito aqui, mas assim, pensem em conversar com o pessoal de projetos, e erros que a gente vê, não é... não cortem verba de segurança, definam requisitos de segurança no início, não achem que vai ter alguém... Tá? Então, esse é um papel de todo mundo na comunidade técnica. Não, não é só botar um firewall depois, não é só botar um antivírus, a gente precisa ter todo mundo engajado em fazer configuração segura, em aplicar *patches*, erro humano. E como eu sei que tem muita gente aqui de... professor de faculdade, Fatec, pessoal que dá aula, pessoal, pensem em segurança desde o início, pensem... se você dá aula de programação, ensina desde o início que tem que checar uma entrada, ensina desde o início que tem que se preocupar com segurança, pensem no pensamento crítico, não criem maus hábitos nos alunos de vocês, não achem que depois alguém vai poder fazer a segurança, porque aí depois é muito mais difícil, não é?

E uma coisa que eu diria para todo mundo da área técnica, pessoal: pensem na parte de ética, na parte de impacto na sociedade, não é? A gente sempre pode ter consequências não previstas e não consideradas aí no que a gente está fazendo do ponto de vista técnico. Não é porque dá para fazer que a gente deve fazer. Eu acho que isso cada vez mais está ficando claro em questões de ciência de dados, de *machine learning*, de uso de inteligência artificial, de quanto você cria um serviço novo. Pense que alguém vai querer abusar essa tecnologia e sempre se pergunte, assim: O que pode dar errado se alguém abusar isso que eu estou colocando no ar agora, pessoal? E engajem-se aí, não é? Todo mundo falou de educação, eu acho que todo mundo sabe que a gente aqui no NIC tem o portal internetsegura.br, que a gente aponta para várias iniciativas do Brasil e nossas aqui, tem o BCP, que é a parte de recomendações técnicas aí para a comunidade técnica, e vamos ver aí como vai ficar a discussão. Eu vi que tem muita pergunta no chat, e espero que a gente consiga, pelo menos, responder algumas. E eu passo de volta aí para o pessoal da organização. Obrigada a todos.

SR. ANTONIO MARCOS MOREIRAS: Obrigado a você, Cristine, pela participação. Antes de ir para as perguntas, eu gostaria de lembrar a todos que temos sorteios, não é? Temos um kit do próprio NIC.br mais patrocinadores, quer dizer, um kit com alguns prêmios oferecidos pelo próprio NIC e alguns patrocinadores. Deixa eu tentar mostrar aqui para vocês. Está aqui atrás de mim, não é, mas eu tirei também... Aqui, olha. Temos esse kit, várias coisas interessantes aí. É um kit que até eu gostaria de ganhar. Infelizmente, não tem aqui para os apresentadores da live, tem para vocês que estão assistindo a live. Então, inscrevam-se. E temos também sorteios dos patrocinadores. Temos, por exemplo, o Netfinders Brasil sorteando uma vaga no curso de BGP + MPLS Avançado no modo gravado, temos a GlobeNet sorteando aí um fone de ouvido sem fio Bluetooth... O que mais temos

aí? Temos a Globo sorteando um voucher da Globoplay com acesso grátis por dois meses, e temos o certificado, não é? Quem precisar de certificado de participação da live, tem que fazer a inscrição no nosso site até às 14h, vai receber um link, tem que como que dar presença, não é, falar que está participando ali, que, de fato, assistiu a live ao vivo, que o certificado é para quem está acompanhando ao vivo, e não para quem está acompanhando em modo gravado. E temos aí... Vamos já colocar aí o QR Code da avaliação. Não estou mandando ninguém embora, a gente ainda vai para a parte das perguntas aqui, mas vocês já têm uma ideia de vocês, se vocês gostaram ou não gostaram da live, já conseguem responder a nossa avaliação. Então, o pessoal vai colocar um QR Code aí no vídeo e vão colocar o link também da avaliação no chat, e a gente pede para todo mundo que está acompanhando a live que avalie. São duas perguntas, não vai tomar nem um minuto do seu tempo. É dar uma nota da live de zero a dez, e se tiver algo que vocês queiram que melhore na live, vocês coloquem lá, façam um comentário, alguma coisa que atrapalhou, tal. A gente já tem ciência da imagem tremida, não é? Se quiserem colocar, podem colocar também, mas coloquem outras questões aí. Como é que a gente pode melhorar para as próximas lives? Então, vocês podem responder isso daí para a gente. Se quiserem só dar a nota de zero a dez, não quiser fazer nenhum comentário, também tudo bem, não tem nenhum problema, certo?

Eu gostaria de começar com uma pergunta mais genérica para o pessoal que está aqui, e daí quem dos painelistas quiser responder... A gente vai perguntando na mesma ordem que vocês fizeram as apresentações. Antes de partir para as perguntas mais específicas aí feitas no chat, o pessoal que está acompanhando ao vivo, se quiser fazer perguntas que ainda não tenham feito, podem colocar aí, continuem colocando no chat, porque a gente está acompanhando, está coletando aqui. A gente, na medida do possível, vai tentar passar essas perguntas para os painelistas. Eu gostaria que cada um falasse de forma bastante breve qual é o principal problema hoje de segurança na Internet, aí na visão do setor, ou mais ligado ao setor ao qual você representa aqui nessa live? Qual que é a principal questão de segurança para a gente tratar na Internet hoje? Parajo, você gostaria de responder isso?

SR. EDUARDO PARAJO: Pode ser, Moreiras. Não sei se eu vou conseguir acertar, mas beleza. Boa pergunta aí, porque assim, como eu comentei na primeira intervenção, eu acho que vários também dos palestrantes também falaram, não é, eu acho que, assim, a gente tem uma preocupação bastante grande com o equipamento, ou com os equipamentos, dos usuários. Isso efetivamente é um *locus*, vamos dizer assim, de possíveis problemas que a gente possa ter de falha de segurança, ou refletores de ataques, ou caras que estão sendo utilizados sem, vamos dizer, sem o mesmo usuário ter ciência de que

ele está tomando ou que ele está contribuindo para o ataque, não é? Então, eu acho que esse talvez seja a nossa maior preocupação hoje, de efetivamente ajudar a... colaborar com esse nosso usuário a estar conectado aí na Internet para que ele possa estar fazendo as atualizações de segurança do seu software, que, dentro do possível, ele tenha uma proteção mínima ali de um software de antivírus que possa colaborar com ele, mas o ponto principal que a gente vê é a falta de atualização, de vulnerabilidades no próprio sistema operacional. Isso é uma coisa que realmente acaba nos preocupando muito.

Um segundo ponto aí que eu acho que a gente tem abordado de maneira bastante eficiente e eu acho que tem tido bastante resultado são aí os equipamentos que estão no próprio usuário também, não só o computador dele, mas tem lá o seu roteadorzinho Wi-Fi, essa coisa toda, e também é um ponto ali de preocupação até para ter efetivamente aí mais segurança e não estar sendo utilizado de forma indevida na Internet. Eu diria que essa preocupação com o usuário, com o usuário estar conectado, que equipamentos ele está usando lá, se os softwares estão atualizados, essa é uma preocupação bastante grande.

Do lado do provedor, é como eu expliquei na minha intervenção anterior, todos que a gente conversa nessa troca de informações ricas que tem hoje no mercado têm atuado de forma bastante forte para seguir as boas práticas de segurança na infraestrutura, para que ele não possa estar vulnerável. Mas, brevemente, eu acho que seriam esses os dois pontos aí.

SR. ANTONIO MARCOS MOREIRAS: Muito bom, Parajo. Não tem acertar ou errar, não é? A gente chamou aqui justamente para a gente se beneficiar da sua experiência, da sua visão, e é bastante interessante. Eu concordo bastante com isso daí, a gente tem esse problema de atualização de softwares, a gente tem a questão da importância de seguir as boas práticas. Mas eu não estou aqui para dar a minha opinião, eu estou aqui para ouvir a opinião também do Cristiano Pimenta, da Claro, se ele puder... se o Cristiano quiser fazer algum comentário sobre isso, de forma resumida, breve, dizer qual que é o principal problema de segurança da Internet a ser tratado, a ser resolvido aí, na visão da Claro e das grandes operadoras de telecom.

SR. CRISTIANO PIMENTA: Obrigado, Moreiras. Olá, pessoal. Moreiras, a abordagem que eu trago não de um problema, mas como um desafio, como foi comentado pelo Parajo, mas eu trago dentro do seguinte contexto: hoje, o usuário, ele tem um grande poder nas suas mãos, um poder de processamento, um poder de acesso à informação, acesso a dados, e administrar esse poder, que passa, como foi comentado também pela Cristine, e a questão da conscientização, isso é um grande desafio, não é? Porque o usuário, hoje, ele pode acessar o que quiser, compartilhar o que quiser, mas precisa se proteger. Ao

fato de não se proteger adequadamente, ele eleva o risco, e muitas das vezes esse risco, ele fica em uma situação ali no meio caminho, não é? A responsabilidade é de quem? Sou eu, usuário, que não protegi o meu WhatsApp, não usei o múltiplo fator de autenticação, um segundo fator, ou cadastrei meus dados em um site que não era um site confiável e, ao fazer isso, gerei uma exposição, e essa exposição, ela é amplificada, não é, e seus dados vazam e você fica exposto. Então, eu diria que um desafio na segurança da Internet, em muitas das vezes ele está muito centrado na questão desse poder que o usuário tem, e nós aí como segmento e parceiros, nós precisamos de fato, junto, inclusive, com o órgão regulador, que tem feito um trabalho bacana com o time da Vanessa, nós temos que potencializar, levar essa consciência e amplificar a proteção de todos os usuários. É um pouco do que eu gostaria de comentar nesse sentido.

SR. ANTONIO MARCOS MOREIRAS: Muito obrigado. Fernando, você gostaria de acrescentar algum comentário? No ponto de vista dos fabricantes de equipamentos, o que é o ponto que pode ser melhor aí tratado, o que afeta mais a Internet?

SR. FERNANDO ZAMAI: Eu vou até acho que pegar o gancho que a Cristine colocou de uma forma muito assertiva. Ela colocou... no meio da fala, ela jogou um termo técnico e também mostrou uma coisa que eu compartilho, não é, que acredito muito: o distanciamento entre governança e o técnico, não é? Existe um abismo entre estabelecer normas e a execução das normas, a ativação de fato daqueles recursos, que aí se esperam, não é, infelizmente, a gente espera que o governo coloque uma normativa para você fazer algo que você já poderia fazer hoje. E, também, colocando a LGPD no contexto, até puxando uma apresentação que eu fiz uma vez na Febraban e estava o promotor público do governo do estado, toda e qualquer... As leis do nosso mundo físico se aplicam ao mundo virtual. Toda e qualquer. Então, qualquer um que se sentir lesado, recebeu um Phishing, clicou, caiu em uma fraude, você tem direito de processar. O que está acontecendo e o que eu vejo na LGPD é que o Judiciário está amadurecendo, o Judiciário está aprendendo a lidar com essas novas questões digitais. Então, se o provedor do seu dado deixou vazar e tem responsabilidade, e você conseguir provar isso, você tem direitos, tá? Então, isso é uma crescente, cada vez mais processos em cima do âmbito digital. E aí, eu vou pegar para mostrar alguns elementos... Eu acredito, assim, como engenheiro, tem alguns parafusos que a gente aperta na Internet que eles surtem um efeito muito positivo, e mais do que outros. Vamos pegar o Spoofing por exemplo. A gente fala de DDos, amplificação de DNS, um monte de coisa. Se você corta o Spoofing na ponta, você já eliminou uma quantidade de sujeira enorme dessa categoria de ataque. E aí, falando de Spoofing, a gente tem o *email spoofing*. E-mail representa, ainda, 92% do problema que afeta a nossa vida, não é? Então, você recebe lá um Spoofing, você já

aprendeu que você tem que verificar o domínio, saber quem é para não clicar e cair na fraude. Aí você recebe um e-mail da sua empresa, da empresa que você tem serviço... do seu banco, por exemplo, você recebe um e-mail do seu banco, vem com o domínio do banco, e você, fazendo o que o usuário tem capacidade de fazer, você verifica, "não, realmente, veio do meu banco, vou clicar", e cai em uma fraude, tá? O fato é... Então, pegando uma tecnologia que a Cristine falou, existe uma técnica para você bloquear Spoofing de e-mail. Noventa e dois por cento das ameaças vem por e-mail. Existe uma tecnologia que autentica a comunicação onde uma empresa garante que só vai mandar e-mail para o domínio dela ela mesma. Ela pode bloquear que alguém use o e-mail dela para disparar Spoofing. Aí a questão é: as empresas contratam esse recurso? Eu, infelizmente, já escutei de grandes empresas que: Ah, legal, bacana, vamos colocar aqui no nosso plano de route-map... Porque o governo americano soltou uma nota que todas entidades do governo, para disparar um e-mail para o cidadão, têm que ter essa tecnologia antispoofing de e-mail. E aí, escutei no Brasil de uma grande empresa: Ah, legal, entendo, estou consciente, tal, está no meu route-map, mas não é prioridade agora, enquanto não for obrigatório, enquanto não vir alguém falar que é obrigatório. Então, isso é um item de responsabilidade que eu acho que vai mudando aos poucos. Então, se você cair em um Phishing que veio de um domínio, que está com o domínio legítimo da empresa que o lesou, você pode abrir um processo, e a LGPD vai levar o tema no Judiciário de uma forma diferente. Então, eu acho que tudo isso junta. Eu acredito que tem alguns parafusos técnicos lá na ponta que podem ser apertados, não é? Muita gente espera uma regulação para entrar em vigor, mas ela pode ser aplicada hoje. A questão é: custa, custa investimento, custa processo, custa pessoas. Então, assim, você tem que investir em tecnologia, processo e pessoas, e esse investimento não é pouco, não é? Então, o pessoal... Hoje, não é, o ciber está ganhando relevância, porque olha o tamanho da fraude. Quanto é que cobraram no último ransomware da empresa que caiu? O tamanho da fraude não é pequeno. E esse orçamento de segurança, que é muito baixo no Brasil, tem que ser repensado e trabalhado de maneira diferente, mas eu vejo um progresso, tudo isso é um progresso, e a LGPD talvez é um dos principais. A Anatel também soltou normativa nova falando de CPE, segurança. Aos poucos vai tocando esses parafusos que vão apertando ali e vão tornando mais seguros.

E tem uma crítica, não é, o pessoal muito falando em pais, privacidade. Eu acho que principalmente as operadoras e o governo têm uma preocupação muito grande em privacidade, não é? Quando se aplica controle, quanto isso afetou na privacidade? Então, você tem que ter um balanço ali do que eu consigo de fato apertar. Mas eu acredito que uma técnica antispoofing, se eu levar... principalmente no e-mail, que é 92% da onde vem as ameaças, eu já tornaria aí mais seguro.

SR. ANTONIO MARCOS MOREIRAS: Muito obrigado. Eu gostaria agora de perguntar para a Vanessa. Vanessa, você gostaria de contribuir com essa questão, de enfatizar algum ponto?

SRA. VANESSA COPETTI CRAVO: Obrigada, Moreiras. Não, acho que foi bastante feliz e desafiadora a pergunta, não é? Eleger um ponto que, digamos assim, concentrasse essa dificuldade, esse desafio, é bastante desafiador. Mas eu queria trazer uma perspectiva. Quando a gente está falando de segurança da Internet, a gente está falando de uma responsabilidade compartilhada, e justamente essa live, a composição da live, ela reflete isso, justamente toda essa representação. Então, digamos assim, o problema, o grande desafio, é fazer com que todos os elos dessa cadeia, eles entendam o seu papel e adotem uma conduta em conformidade com esse papel que ele tem na rede, e por isso a importância da conscientização, que apareceu em todas as falas anteriores, não é, [ininteligível] as apresentações e o ponto de conscientização, e até mesmo agora, já nessa resposta, já apareceram novamente. E nisso, o regulador, ele tem um papel fundamental para que o setor reconheça a sua responsabilidade, não é? O regulador reconhecendo a sua responsabilidade nesse ponto, ele tem que fazer com que o setor também aja em conformidade. E nisso, a questão do fomento às boas práticas e a adoção de padrões necessários, daí a gente pode também já ir chamando a fala do Fernando também olhando para questões técnicas e específicas desses padrões e requisitos, e pode ser feita de uma forma mandatória, como fez através de regulamentação, o Regulamento de Segurança Cibernética, um ato a eventuais ações adicionais concretas para que o setor aja em conformidade, ou mesmo criando um ambiente, um ambiente de construção coletiva também para que o setor possa dar a sua contribuição, e nisso, a Anatel e o setor como um todo já têm mostrado esse comprometimento e estamos empreendendo esforços nesse sentido, que não é fácil, é um desafio bastante ambicioso, mas estamos comprometidos com isso. Obrigada.

SR. ANTONIO MARCOS MOREIRAS: Obrigado você, Vanessa. Alê, você quer comentar?

SR. ALÊ BORBA: Bom, Moreiras, o meu ponto aqui, ele é bem similar, eu acho, ao do Parajo, não é? Eu acho que o grande desafio hoje da segurança na Internet é que essa educação digital de segurança digital chegue para todo mundo, sabe, porque hoje os maus atores, eles se aproveitam dessa falta de conhecimento que os usuários, ou as pessoas, têm sobre algumas questões de segurança para agir, sabe? Então, hoje, por exemplo, uma das principais formas de golpe hoje é a engenharia social, que pode, teoricamente, ser facilmente... não facilmente, mas ela pode ser minimizada, os efeitos dela, se você tiver essa educação social, como já foi colocado, de não clicar em qualquer coisa que te mandam e pesquisar mais e saber mais o que está acontecendo, sabe, antes de passar uma informação ou

qualquer coisa do tipo. Então, acho que hoje, para esse nosso setor de conteúdo, eu acho que um dos principais desafios é que essa educação digital chegue para todas as pessoas e alcance o maior número de pessoas possível. A gente tem trabalhado muito nisso, todo mundo tem trabalhado muito nisso. Isso você tem... a gente tem visto cada vez mais aí na mídia aberta, inclusive, pessoas falando, dando entrevistas sobre isso, que é muito importante, mas ainda é um desafio muito grande para todo mundo.

SR. ANTONIO MARCOS MOREIRAS: Muito obrigado. Cristine, você quer fazer algum comentário rápido?

SRA. CRISTINE HOEPERS: Bem rápido. Eu acho que em cima disso que o Alê comentou, que ele falou, assim, o papel social, não é? Eu acho que uma coisa que a gente precisa fazer, independente de qual é o nosso setor, é pensar que você tem que fazer alguma coisa que melhore a Internet, mas que talvez, não necessariamente, vai melhorar o seu ambiente, a sua segurança. Eu acho que antispoofing, seja adotar tecnologias como DMARC, DKIM, que vão proteger o seu usuário, mas não necessariamente a sua conta de e-mail, e antispoofing nas redes, quer dizer, a gente implementar antispoofing para reduzir DDoS, para impedir que alguém ingere pacotes privados, o incentivo, ele não existe para quem implementa isso, não é? O incentivo é de você contribuir com a Internet, de você evitar que pessoas sofram Phishing porque usaram a marca da sua organização, o seu @empresa, @governo, para mandar um Phishing, ou que saiu um pacote 'spoofado' da sua rede, e aquele pacote 'spoofado' que conseguiu fazer o disparo em uma botnet, atacando uma vítima. Então, eu acho que, assim, é pensar que... você tem que pensar nos incentivos, que eles... nem sempre você vai colher os frutos, mas você precisa que todo mundo faça para que todo mundo tenha um pouco mais de segurança, e aí que vem a importância de todo mundo pensar em senha, todo mundo pensar em segundo fator, todo mundo ajudar a educar o usuário, todo mundo fazer um pedaço desse papel aí, porque não vai ter ninguém que consiga resolver o problema sozinho, não é? Era esse o meu comentário aí. Obrigada.

SR. EDUARDO BARASAL MORALES: Obrigado, Chris. Bom, a próxima pergunta é uma pergunta relacionada à LGPD. Veio muita discussão aí no nosso chat relacionada à LGPD, o pessoal está com dúvida, e aí a gente queria saber: Como a LGPD pode afetar aí o seu setor? Então, venho pergunta do Mesaque, do Tem Rede Aí, da Nelci, do Ulisses, e a gente vai tentar aí compilar essas perguntas para os nossos palestrantes.

Então, queria chamar agora o Eduardo Parajo. Parajo, como é que você acha que a LGPD está afetando os pequenos provedores, provedores regionais, as pequenas prestadoras de telecomunicações? E aí, eu queria até já puxar um linkezinho também, além de você falar

geral, eu gostaria de puxar o link para o Tem Rede Aí, que ele perguntou ali: Olha, eu estou fornecendo uma VPN com criptografia fraca, porém, com serviço gratuito. Caso eu seja atacado e os dados sejam expostos, eu sou o responsável? Então, pensando ali que você está provando outros serviços para o seu cliente, se acontece alguma coisa, e é de maneira gratuita, você é responsável também? Então, queria que você falasse do setor, e se pudesse tocar um pouquinho nesse assunto também ficaria interessante. Então, fique à vontade, Parajo.

SR. EDUARDO PARAJO: Obrigado, Eduardo. Bom, a LGPD, realmente, é um tema importante e que deve ter atenção, sim, dos provedores e das pequenas prestadoras de telecom, não é? Basicamente, os provedores, hoje, coletam informações dos clientes muito exclusivamente para efeitos de cobrança, de cadastro e coisa desse tipo, mas é importante, sim, ver a regulamentação, é importante seguir e criar uma política de segurança dentro do provedor, uma política sobre como ele vai tratar esses dados, de que forma que ele vai armazenar esses dados, quem vai ter acesso a esses dados. Então, assim, apesar de ele não ser... vamos dizer assim, não estar manuseando dados de terceiros ou coisa desse tipo, que são talvez os pontos mais críticos da lei, ele, obviamente, tem que tomar todo o cuidado e toda a atenção necessária que a lei exige com relação a como ele vai tratar os dados dos seus clientes, não é? É importante chamar atenção disso. A gente sabe que muitos provedores já têm feito um trabalho nesse sentido, de criar... comunicar as suas políticas de segurança e tudo o mais. A gente também sabe que tem uma exceção na lei com relação às pequenas e médias empresas, que é importante nesse sentido de você ter uma simetria nesse processo, na lei geral, mas chama atenção aí, e reforço o ponto de que sim, os provedores têm que estar atentos à questão da Lei Geral de Proteção de Dados para evitarem maiores problemas, não é?

Bom, com relação à questão técnica aí do serviço que é ofertado, como é ofertado e tudo o mais, esse é sempre um ponto de atenção necessário, para quem está prestando o serviço deixar muito claro para o seu cliente o que ele está fazendo, quais são as condições da prestação de serviço, o que ele está entregando para o cliente e tudo o mais, porque muitas das vezes a gente acaba vendo que o pessoal ou vai no grátis, ou vai no mais baratinho possível, o que custa menos no geral, e isso pode, sim, trazer problemas, mas eu acho que, assim, se deixar muito bem claro a regra do jogo, qual é o jogo está sendo jogado, o que está tendo... o que está sendo oferecido, eu acho que aí você vai evitar maiores problemas e maiores confusões depois, em qualquer vazamento de dados ou coisa desse tipo. Eu vejo que hoje as empresas, em geral, se esforçam bastante, os provedores se esforçam bastante no sentido de tentar cada vez deixar mais claro para o cliente qual é a oferta que ele está fazendo, o que ele está entregando naquela

oferta, detalhando isso para que a coisa fique muito clara. Obviamente que a gente sabe que às vezes também o cliente acaba não se atentando aos detalhes, o que ele está contratando, e, às vezes, pode até estar contratando um gato por lebre, vamos dizer assim, mas eu acho que é importante a gente deixar nas ofertas que são feitas ao cliente final o mais claro o possível o que ele está comprando, bem esclarecido, para que a gente possa evitar problemas com a LGPD, problemas com o próprio serviço no geral, que eu acho que isso é bastante prejudicial para todos, não é? Lembro: a gente está falando sobre segurança nesse painel hoje aqui. Então, assim, tudo o que a gente fizer no sentido de melhorar a segurança da infraestrutura do provedor, das pequenas prestadoras e dos nossos usuários, isso vai contribuir para a Internet como um todo, vai melhorar a segurança da Internet como um todo. E a preocupação com o usuário é sempre primordial por causa... que a gente sabe que muitas das vezes não tem um conhecimento tecnológico muito grande, acaba cometendo alguns erros ali de manuseio da tecnologia, e isso pode gerar problemas graves aí, como todos já comentaram durante o painel.

SR. EDUARDO BARASAL MORALES: Obrigado, Parajo. Bom, seguindo aí, Cristiano, gostaria de saber como é que a LGPD afeta o seu setor, e aí eu queria puxar uma pergunta do Mesaque, que ele até fez uma coisa mais direcionada à Claro, não é? Ele queria saber: Um ex-cliente da Claro pode pedir a remoção do seu cadastro pela LGPD? E aí, se você puder falar genericamente sobre... como a LGPD afeta o seu setor e, depois, dar uma pincelada nisso aí, eu ficaria muito grato. O palco é seu.

SR. CRISTIANO PIMENTA: Legal. Obrigado pela pergunta. O contexto da LGPD no nosso segmento de telecomunicações tem uma dinâmica fantástica, não é? Acho que esse é um grande desafio. É um segmento que possui, pela sua própria necessidade, muitas informações, muitos dados, e isso traz um desafio de mapeamento, de proteção, de meios para interagir com o próprio usuário, o consumidor. Então, isso tem sido uma dinâmica muito importante. Trouxe também necessidade, e foi comentado há pouco aqui, de muitos investimentos, investimento em uma infraestrutura, na própria criação da área do DPO, do responsável por isso, pela proteção de dados, o fortalecimento do CDO, que é o chefe de dados, o escritório de privacidade, o *privacy by design*. Então, trouxe diversas dinâmicas para dentro da organização que demonstram, obviamente, que a empresa, ela vem seguindo, junto, inclusive, com o órgão regulador e amparada pela própria lei, muitas iniciativas nesse sentido de cada vez mais proteger, não é? Desafios são muitos, mas nós estamos nos esforçando para cada dia mais, junto com o próprio segmento, não é, atuar de forma muito... não só proativa, mas também identificar qualquer *gap* que surja para poder agir.

Em relação à outra pergunta, que fala sobre a questão do esquecimento, eu diria, não é, talvez seja isso, o direito do esquecimento, no caso da Claro, e aí fico à disposição para quem quiser e puder consultar, nós temos o portal de privacidade, e dentro do contexto da lei, que define como é esse processo para a sua solicitação, ou de esclarecimento de que informação, dado pessoal seu tem dentro da empresa, solicitação do esquecimento, entre outras questões que a lei prevê, neste portal de privacidade nós colocamos à disposição da sociedade, dos nossos consumidores para que possam usar, solicitar informações, tirar dúvidas e também, em caso de eventual necessidade, de informar alguma denúncia, algum fato que tenha trazido algum prejuízo, algum vazamento, e lá também indicamos qual é o canal, ou os canais, não é, que são diversos, desde ouvidoria, desde o canal de segurança, desde o canal da própria privacidade, para que o nosso consumidor se sinta confortável em solicitar informações e registrar uma denúncia para que nós possamos também atuar. Eu agradeço a pergunta, inclusive.

SR. EDUARDO BARASAL MORALES: Obrigado, Cristiano.

Bom, seguindo aí, agora eu gostaria de perguntar para o Fernando, da Cisco. Então, como a LGPD afeta o seu setor, o setor dos fabricantes? E aí, eu também queria pincelar, também, com uma pergunta da Nelci, que ela fala: Qual é a responsabilidade se o equipamento vulnerável causou dano financeiro, moral? Como é que fica nesse caso? Existe alguma coisa na LGPD com relação a isso? Então, fica à vontade.

SR. FERNANDO ZAMAI: Legal. Vamos lá. Quando a Cisco, ela passou pela LGPD, um pouco antes, que a LGPD, ela faz um espelho muito com a GDPR, que é a lei europeia, e vou dar um exemplo de algumas coisas que aconteceram, tá? Porque eu tinha acesso a qualquer chamado de cliente, não é? Então, quando o cliente abria um chamado para um problema de algum produto, eu tinha acesso ao chamado e conseguia ler as informações do chamado. A partir do momento que foi implementada a LGPD, eu passei a não ter mais esse acesso, não é? Então, por que o Zamai, líder de cibersegurança, quer saber do problema técnico do cliente? Eu estava querendo ajudar o meu cliente a resolver o problema, mas eu não tive mais acesso. Por exemplo, a configuração do roteador do cliente está no chamado. Eu poderia entrar e pegar, não é? Então, eu passei a não ter mais esse acesso, e se eu quisesse realmente entrar, eu teria que pedir uma aprovação em vários níveis dentro da empresa. Então, estou gerando uma evidência, uma evidência do porquê você quer ter acesso ao conteúdo da empresa, tá? Então, isso é uma coisa interna, que foram reestruturados todos os sistemas, para poder prover... se adequar à normativa, bem como toda uma interface com o usuário, com o usuário final, e os clientes para você fazer a limpeza de dados, solicitação de informação. Então, existe um movimento chamado *trust*. Até esqueci

de citar, que é o *trust*... internamente você chama de *trust*, mas você... Por exemplo, qualquer protocolo que o equipamento fala dentro da sua rede e a finalidade daquele protocolo, nós entregamos todas as informações do que ele faz ali dentro: Olha, estou comunicando canal de comunicação para fazer *update*, estou fazendo isso... não é, então, o login dos usuários, foi feita toda a tratativa para se adequar à normativa de criação de conta, gestão da identidade, armazenamento dos dados. Então, como empresa, a gente já passou por essa transformação puxado pela GDPR. Então, quando veio a LGPD, isso ficou mais simples. E, lógico, armazenamento de dados no país... então, muitas das soluções hoje, elas são nuvens, não é? Então, uma das coisas que vem beneficiar a segurança é você fazer o consumo como *software as a service*. Por quê? Porque aí isso passa... a responsabilidade da vulnerabilidade passa a ser do provedor, não é? Então, ele que tem que atualizar, ele que tem que manter.

Sobre o equipamento ter vulnerabilidade e isso causar um impacto é uma discussão que está na mesa. Então, assim, o fabricante demonstrando que tentou aplicar todas as ferramentas, que notificou, que avisou, que corrigiu, que se importou, também é levado em consideração na LGPD, não é? Então, uma empresa... Vamos supor, aconteceu um vazamento de dados, [ininteligível] vazamento de dados já vai desmontar(F) a empresa, a empresa vai dizer: Olha, eu investi, eu fiz, eu me preocupei, eu mostrei responsabilidade sobre o tema e atuei. Isso é ponderado até quando a gente entra em discussões de multas, e o Judiciário vai levar isso em consideração, tá?

SR. EDUARDO BARASAL MORALES: Obrigado, Fernando.

Bom, seguindo, Vanessa Copetti, da Anatel, bom, queria que você comentasse um pouquinho aí como é que a LGPD afeta o seu setor, até veio uma pergunta do Ulisses Janssen falando: Qual é a relação da Anatel com a ANPD? Então, você poderia explanar para a gente?

SRA. VANESSA COPETTI CRAVO: Com certeza. Obrigada pela pergunta. Bom, então, em primeiro lugar, é importante ressaltar que a questão da privacidade dos dados dos usuários e também do sigilo das comunicações, ela não é uma novidade para a Anatel. Então, assim, é uma questão de extrema relevância que há muito tempo já é tratada no setor, as regulamentações garantem esses direitos aos usuários, mas, obviamente, a LGPD, como foi bem falado pelo Cristiano, ela traz toda uma nova roupagem, um novo arcabouço que já foi implantado pelas prestadoras, não é? Mas quando a gente fala de proteção de dados pessoais, é importante ressaltar que a gente tem uma intersecção bastante importante relacionada à segurança. Não tem como a gente falar de proteção dos dados sem falar de segurança. Não há dado aí protegido sem essa etapa anterior. E nesse sentido, no Regulamento de Segurança Cibernética da Anatel, que foi aprovado

expressamente, conta como diretriz para orientar a atuação de todas as prestadoras, independentemente do porte, justamente que as suas ações em segurança cibernética sejam guiadas pelo respeito e promoção da proteção dos dados pessoais. E, além disso, uma questão bastante importante no tocante a reporte de incidentes relevantes à agência também exige o reporte de vazamentos de dados, dados dos usuários, ainda que haja esse reporte à ANPD. Então, assim, é bastante pertinente a pergunta, não é, que pergunta a relação da Anatel com a ANPD. Então, nós temos, obviamente, uma relação institucional entre as duas agências, uma relação de cooperação, que também está nesse processo de amadurecimento, como a ANPD vai trabalhar com todos esses órgãos, com todas as agências reguladoras, e também temos uma relação à nível técnico, não é? Por exemplo, quando a gente estava nesse debate internamente no subgrupo técnico de compartilhamento de informações e boas práticas, a gente também fez reunião técnica justamente porque a ANPD também estava nesse processo de discussão do reporte de incidentes, e a gente queria entender como eles estavam para também ajudar no nosso processo, não é? Então, estamos em uma relação que está evoluindo à medida que a ANPD também está se consolidando com todos seus normativos e que ainda deve amadurecer em vários espectros, visto que nós temos essa atuação concorrente com relação a essas regulamentações. Nós temos regulamentações específicas que também envolvem aspectos relacionados à proteção de dados pessoais e, obviamente, tem toda a competência da ANPD nesse sentido. Então, estamos trabalhando em conjunto.

SR. EDUARDO BARASAL MORALES: Muito obrigado, Vanessa.

SRA. VANESSA COPETTI CRAVO: Obrigada.

SR. EDUARDO BARASAL MORALES: Obrigado.

Bom, vamos seguindo aí. Alê Borba, do Google, poderia comentar um pouquinho aí sobre os provedores de conteúdo, como é que vocês enxergam essa questão da LGPD, como é que isso daí pode afetar vocês? Fica à vontade.

SR. ALÊ BORBA: Claro, claro. Então, na verdade, assim, a LGPD foi uma regulamentação muito bem-vinda por todo mundo, assim, a gente vê com bons olhos. Como o Zamai já tinha colocado também, é uma lei que é bem espelhada na GDPR. Então, a gente acha que realmente é uma coisa que veio para ajudar todo mundo e colocar aí em prática os compromissos do setor, não só do Google... especialmente do Google, mas não só do Google, com a parte aí de privacidade e proteção de dados, colocar tudo isso em primeiro lugar. Então, eu acho que ela veio para realmente ajudar nisso e reforçar esse compromisso aí de todo mundo nessa parte. De novo, uma regulamentação, no nosso ponto de vista, muito, muito boa e muito importante.

SR. EDUARDO BARASAL MORALES: Obrigado, Alê.

Cristine, gostaria de complementar e finalizar essa questão aí da LGPD? Fica à vontade.

SRA. CRISTINE HOEPERS: Pode ser. Eu acho que o pessoal já acabou falando tudo, não é? Eu vejo que... uma confusão que acabou sendo criada um pouco é exatamente isso, porque... de incidente, não incidente, segurança, o que é proteção de dados, não é, mas eu acho que o principal a pensar é que para evitar exposição de dados você precisa ter segurança da informação. Então, eu acho que é investir em tudo o que a gente está falando aqui de tecnologia, de uma boa análise de risco e segurança, e a parte dos incidentes, não é, o que a gente vê é que cada vez mais a gente tem a necessidade de ter transparência, porque não tem o certo ou errado e é impossível não ter incidentes. A gente tem que assumir que esses incidentes vão ocorrer. E o que a gente vê é cada vez mais vindo regulações, ou leis, que pedem que isso seja transparente, não é? Então, eu acho que todo mundo tem que estar preparado para mapear, para detectar incidentes acontecendo nas organizações. Vão ter aqueles que têm baixíssimo impacto em cima de dados, ou em cima do serviço, mas aqueles que tiverem, precisam ser reportados, precisam ser trazidos à luz, e precisa avisar os titulares de dados, e precisa avisar todo mundo que ocorreu o problema. Eu acho que esse é o ponto principal, é pensar que para fazer isso da melhor maneira é estar preparado para qualquer incidente, é ter um processo para detectar, para lidar com isso, e assumir que isso vai acontecer, não é, não ser pego de surpresa. Mas era só esse comentário aí que eu tinha para fazer, e vou passar a palavra aí para o pessoal da organização. Eu acho que o Moreiras deve falar, ou o Eduardo.

SR. ANTONIO MARCOS MOREIRAS: Eu, Cristine. Obrigado.

Eu quero chamar o Alê Borba. Tem uma pergunta específica para ele, e ele também já vai ter que se ausentar aqui. Então, eu vou fazer a pergunta, a pergunta do João Alberto Bendlin Junior, se o Google tem plano, visão, de lançar algum serviço ao estilo do FamilyShield, e eu já convido o Alê Borba para fazer as suas considerações finais.

SR. ALÊ BORBA: Claro. Obrigado. Obrigado aí pela pergunta também. Bom, essa pergunta, ela é bem interessante. Eu não sou muito familiarizado, assim... conheço o FamilyShield do OpenDNS, mas eu não estou totalmente familiarizado com ele, mas o que a gente tem hoje... a gente já tem alguns serviços que fazem a mesma... que têm a mesma ideia, não é, por exemplo, como eu já citei, o Family Link, você já consegue fazer... Porque, na verdade, o FamilyShield, assim, até para dar uma pincelada para quem não ouviu falar, ele praticamente cria uma lista de sites bloqueados, que impede o acesso a alguns sites e tudo o mais na configuração do DNS, se não me engano aqui. Eu posso estar, de alguma forma, enganado, mas que eu me

lembre é isso aí. E você pode... Na verdade, o que a gente tem hoje, várias coisas, vários produtos que podem ser colocados... Então, por exemplo, o Family Link mesmo, porque quando se fala de bloquear sites em casa seria mais para um acesso indevido de uma criança, do adolescente, alguma coisa assim. Então, o Family Link, ele vai até um pouco além, na verdade, disso. No Family Link, você pode controlar, inclusive, o que essa pessoa, a criança no caso, ou o adolescente que tem essa conta vinculada, ela instala no celular. Então, ela, por exemplo, ela não consegue fazer pagamento, tem que ser autorizado, o aplicativo que ela vai baixar tem que ser autorizado, o horário que ela vai usar esses aplicativos é autorizado. Então, vai um pouco além aí de só bloquear determinados sites, tá? Então, nesse sentido a gente já tem aí o Family Link. E aí, outras coisas também que a gente já tem aí como... nas contas de crianças e adolescentes, como o SafeSearch, ele é ativado... a busca segura é ativada por *default*, por padrão, e outras coisas que a gente lançou agora, ultimamente. Então, isso aí é uma coisa que a gente tem, e sempre é uma coisa que a gente vai evoluindo. Então, se você quer ficar ligado nos lançamentos dessa parte de segurança, a gente tem sempre lançando coisas novas aí.

E para fechar, queria agradecer de novo aí o convite de todo mundo, e, assim, falar que esse tipo de iniciativa que o NIC está tendo é muito importante, trazer todo mundo para a conversa, e, assim, reforçar o quanto é importante que a gente continue com esse... pelo que a gente percebeu aqui, não é, podemos perceber na live, todos os setores estão engajados aí nessa educação digital do usuário, e é muito importante a gente continuar fazendo isso. E quem está assistindo hoje, se puder continuar espalhando essa palavra, sabe, da segurança, das senhas e de todos... de como isso funciona, de como isso é importante, isso é muito bom, porque eu já escutei, por exemplo, pessoas falando: "Eu não tenho senha no meu celular, porque no meu celular não tem nada". E, poxa, gente, a gente sabe que não é bem assim. Quando você começa a perguntar, você fala: Poxa, mas o seu e-mail está logado, mas o seu WhatsApp está logado... Aí você começa a ver, a pessoa fala assim: "Nossa, realmente, eu acho que tenho muita coisa no meu celular". Então, a gente tem que continuar reforçando a importância disso e trabalhando aí junto com todas as áreas da indústria, e, como eu falei aqui, não existe concorrente nesse setor, nessa parte de segurança, a gente só tem parceiros, continuar trabalhando juntos para cada vez mais a gente conseguir impedir que esse tipo de ameaça se espalhe na Internet. E é isso. Muito obrigado novamente pela oportunidade e pelo convite.

SR. ANTONIO MARCOS MOREIRAS: Nós é que agradecemos, Alê, é um prazer ter você aqui, um prazer ter o Google participando também institucionalmente e você, pessoalmente, aqui conosco. Muito obrigado.

Eu gostaria agora de chamar o Cristiano Pimenta. Tem duas perguntas aqui específicas, não é, e depois eu vou pedir também que o Cristiano faça as suas considerações finais aí, que gostaria de acrescentar para a gente. Então, tem uma pergunta do Anderson Figueiredo, que é sobre como a Claro vê o *security by design* para os seus produtos, e tem uma segunda pergunta, que é do Octaiver Matt, que pergunta aqui quanto tempo a Claro guarda os Logs do CGNAT e os Logs do CGNAT que está fazendo para o virtual. Quanto tempo a Claro está guardando os Logs do CGNAT? Então, Cristiano.

SR. CRISTIANO PIMENTA: Ok, vamos lá. Vamos acertar(F) em relação ao Log, não é? Em relação aos Logs, no caso que eu opto por não indicar exatamente o tempo, mas que nós temos, por premissa legal, a guarda de Logs de diversas definições legais, seja para investigação, atendimento a regulador, não é? Teve perguntas também relacionados à LGPD, não é, que na própria lei, ela não definiu o tempo, mas você tem que atender o tempo de cada demanda específica. Então, se você tem informações tributárias, você tem um determinado delta T para guardar, informações para efeito judicial, investigativo, você precisa ter esse tempo. Para efeito específico dessa pergunta, nós guardamos o tempo que é o tempo necessário que a lei ou a solicitação legal define. Pode ser que cinco, dez anos, ou um pouco mais, ok? Moreiras, qual era a outra?

SR. ANTONIO MARCOS MOREIRAS: A outra... deixa eu ver aqui também. A outra é sobre *security by design*.

SR. CRISTIANO PIMENTA: Isso.

SR. ANTONIO MARCOS MOREIRAS: É.

SR. CRISTIANO PIMENTA: Essa é interessante. A gente vê hoje uma integração muito interessante, eu diria assim, muito produtiva entre o contexto e o conceito do *security by design* e a própria questão do *privacy by design*. Então, hoje, na Claro, nós estamos caminhando para essa sinergia, e existem muitas empresas nos ouvindo aqui, é muito importante que você defina esse modelo de integração, que nós chamamos aqui do *privacy by design*, desde o nascimento de um serviço a um produto, onde você conecta todas essas interfaces de negócio, de segurança, de privacidade, de arquitetura do dado, de arquitetura da solução, e em uma esteira organizada e controlada, você vai definindo e acompanhando o atendimento de requisitos, tanto de privacidade quanto de segurança. Olhar hoje só para o *security by design* sem ter esse olhar da privacidade, me parece que isso acaba gerando um *delay*. Nós optamos por seguir em conjunto em uma sinergia dentro de um processo já organizado, sistematizado, que garante... com *workflow*, que garante, principalmente para que [ininteligível] os produtos e serviços novos, não é, porque a gente tem... como qualquer empresa, existe o seu legado, não é, para os produtos e serviços novos entrarem nessa

esteira e seguirem de uma forma bastante produtiva e interessante, que também foi a fala da Vanessa, dessa integração entre segurança e privacidade, eu acho que a Cristine também falou sobre isso, que tinha... logo no início a gente tinha essa dúvida entre o que são incidentes de privacidade ou incidentes de segurança, mas isso é quando já é um incidente, não é? E quando está nascendo um produto e um serviço? Não dá para ficar separando o que é segurança e privacidade, tem que implantar isso dentro de um contexto só, e nós, hoje, estamos organizados para tratar desta forma.

E aí, eu aproveito para fazer esse fechamento. Você que está nos ouvindo, você faz parte dessa realidade, não é? Foi comentado aqui há pouco pela Google, você tem um celular e não protege, ou você tem uma senha e ainda escreve no Post It, e você compartilha, você fala coisas no lugar errado, compartilhando o seu dado pessoal, cadastra no site que não devia, você faz parte dessa realidade, e essa realidade, também já foi comentado dessa dinâmica das ameaças, da criatividade do crime, em tentar obter de qualquer forma um dado pessoal para cometer outro crime em teu nome, eu chamo atenção para que você compartilhe, amplifique esta mensagem, essa oportunidade que o NIC.br está trazendo, e acredito que teremos outras, não é, de uma forma massificada levar o conhecimento, levar a informação para o cidadão para que ele também possa se sentir integrante não só na hora de reclamar que foi invadido, ou reclamar que perdeu um determinado valor na conta bancária que foi invadida, mas que ele também entenda que ele é parte da solução, e ele precisa estar ciente disso e integrado, não é, buscar informação, denunciar, ajudar a buscar a solução. Essa é uma mensagem que eu gostaria de deixar, Moreiras.

SR. ANTONIO MARCOS MOREIRAS: Muito bom, Cristiano. É bem interessante isso, porque a gente chamou os diversos setores aqui e a gente não chamou os usuários, não é, e todos, no final, somos usuários da Internet, e como cada setor tem a sua responsabilidade e a sua participação no sentido de aumentar a segurança da Internet, nós, como usuários, e os usuários em geral da Internet, também têm a sua participação e o seu papel nisso, não é? Eu vou aproveitar até para... vou fazer o jabá do nosso próprio produto aqui, do Cidadão na Rede. Depois, no final, a gente vai colocar outro videozinho, que é uma das iniciativas em que o NIC.br tenta levar, vamos dizer assim, conhecimento para o usuário leigo sobre como ele pode usar a Internet de uma forma melhor, mais segura, e eu sei que tem várias iniciativas desse tipo. Isso é muito importante, é muito importante que os usuários também assumam s seus papéis. Não é a questão de a gente querer, vamos dizer assim, tirar a nossa responsabilidade, jogar a responsabilidade para os nossos clientes, para os nossos usuários, muito longe disso, não é? Cada setor aqui falou muito bem sobre o seu papel, sobre as responsabilidades que tem assumido, mas tem também essa questão dos usuários. Então, muito obrigado pela participação,

muito obrigado pela sua participação pessoal. Eu deixo aqui agradecimento para o Paulo também, que participou, e a participação institucional da Claro aqui na nossa live. Agradeço bastante.

E aí, eu gostaria de chamar o Parajo. Parajo, tem uma pergunta aqui também específica, essa eu nem avisei para você antes porque é uma pergunta... eu acho que é simples, mas o Sergio Eduardo Antonio perguntou o que está acontecendo com o ping, com o ICMP, e eu acho que você talvez consiga dizer alguma coisa. A gente não sabe. Ele está sendo barrado, bloqueado? Mas o que eu gostaria mesmo... Então, se você quiser fazer algum comentário sobre o ping, o ICMP, ou bloqueios na rede em geral, mas eu gostaria mesmo de chamar você para fazer as suas considerações finais.

SR. EDUARDO PARAJO: Bom, Moreiras, eu não sei exatamente qual que é a pergunta, mas eu vou levar ela no contexto da segurança, tá? Na verdade, os usuários, em geral, utilizam bastante a ferramenta do ping, não é, do ICMP aí para verificar latência dos seus destinos ou coisa desse tipo. Só lembro a todos que isso também é utilizado como técnicas de ataque, não é, você gerar um volume astronômico aí de pacotes ICMP com destino a um equipamento, um roteador, um servidor ou coisa assim. Então, normalmente, o pessoal do contexto aí da segurança faz bloqueios de segurança, principalmente em ativos de conectividade, switches, roteadores e tudo mais, e esses ativos, eles, obviamente, ficam mais suscetíveis e mais expostos à Internet como um todo. Então, o pessoal faz bloqueio, sim. E não só faz bloqueio em determinados pontos mais críticos, que não respondem ao ping, como também fazem, dependendo, por exemplo, de um site ou coisa assim, eles fazem uma limitação da quantidade de pacotes que eles vão receber, não é? Então, efetivamente, esse é o contexto da segurança, vamos dizer assim, e é importante observar. E, às vezes, a gente tem até problemas com isso. Os usuários, às vezes, acabam reclamando quando algum desses limites alcançado e começa a perder, vamos dizer assim os pings, o pessoal acha que, na verdade, está perdendo a comunicação e que isso é um problema. Então, tem outras maneiras de auferir essa comunicação, de verificar isso, que a coisa está estabilizada e que está funcionando, e aí o pessoal entender que, na verdade, boa parte dessa questão é relacionada à segurança, quer dizer, para você evitar aí comprometimento de roteadores, de switches e tudo o mais que estão conectados à Internet. Acho que era isso que, talvez, no contexto é a resposta para essa pergunta.

Agora, aproveito, então, já para me despedir também. Agradecer a toda a equipe do NIC. Acho extremamente relevante esse tipo de debate que a gente está tendo aqui hoje, trazendo mais informações para os usuários, tendo a indústria reunida, desde conteúdo, provedores, grandes operadoras, pequenas operadoras, a Anatel e o próprio NIC envolvido aí com os especialistas aí, o Moreiras, o Eduardo e a Cristine, principalmente, na área de segurança, e reforçado a

importância desse tipo de evento on-line para que a gente possa cada vez mais estar colocando essa informação de maneira acessível aos usuários finais, para que se entenda um pouco mais do que rola além das linhas ali do acesso à Internet, da conectividade de Internet, e tem um contexto bastante grande colaborativo de toda essa cadeia aí envolvida em prestar um bom serviço de Internet, uma conectividade de Internet muito boa. Parabéns mais uma vez aí pela iniciativa do NIC, e obrigado pelo convite, Moreiras.

SR. ANTONIO MARCOS MOREIRAS: Nós é que agradecemos, Parajo. Eu acho que você contextualizou perfeitamente a pergunta do Sergio Antonio.

E vamos lá, eu gostaria de chamar o Zamai. É isso mesmo, o Fernando Zamai. Fernando, também tem uma pergunta específica para você, do Paulo Santos. Ele falou aqui, ó: Prof. Zamai, em 2000 a Cisco afirmou que haveria um déficit violento de especialistas em rede nos próximos quatro anos, quer dizer, 2000/2004. E daí ele queria saber se a Cisco sanou esse problema, ajudou a sanar esse problema, se isso de fato aconteceu, ou se ela colocou mais inteligência nos equipamentos e agora a gente não precisa mais de especialistas em rede. Então, se você quiser comentar isso, você comenta, mas eu gostaria mesmo de convidá-lo para fazer as suas considerações finais sobre o assunto da nossa live aqui. Fica à vontade.

SR. FERNANDO ZAMAI: Não, legal. Então, uma pergunta muito boa essa, não é? Em 2000... Eu acho que foi sanado. Eu fui formado em redes pela Academia Cisco nessa época, não é? Não comecei na Cisco, mas hoje a gente tem bons profissionais de rede. O que vem acontecendo é que a simplificação para ativar a tecnologia coloca em evidência se a empresa precisa de um profissional do tipo CCE, não é? Eu acredito que sim, as empresas e, principalmente, os provedores precisam dos bons profissionais de rede, tá, eles não morreram, e não vão morrer, que, no final, mesmo que seja simples a ativação de uma tecnologia, por baixo tem um protocolo, e eu preciso de um profissional que entenda como aquele protocolo funciona, como eu protejo aquele protocolo, como foi citado pela Cristine, por exemplo, IPv6, então toda essa tecnologia, isso ainda precisa. O que acontece hoje é que existem... os profissionais de redes são mais comuns, profissionais de segurança eu acho que a gente está na mesma página de 2000. Então, começamos agora com a Academia de Cibereducação para iniciar a formação em segurança desses profissionais e alimentar o mercado, não é? Então, é um mercado que está mais aquecido, o de ciber. Eu até convido os profissionais de rede que tiverem interesse de se especializar em segurança, de partirem para essa jornada, porque é uma área que vem crescendo muito forte, não é, vide a live que a gente está fazendo aqui. Então, eu acho que redes é a base, eu acho que é o fundamento, e compreender bem esse fundamento ainda é extremamente importante, e o profissional de segurança, ele vai

adquirindo mais conhecimento em cima disso, não é? Os especialistas de rede sabem como afetar os protocolos, sabem como derrubar se não ativar a segurança, e esse conhecimento deles é extremamente valioso para montar uma estratégia de defesa. Então, essa formação, ela é promissora, tá? Então, acredito que em 2000 sim, foi sanado, tanto que a Internet está aí funcionando em alta velocidade, não é? Eu acho que a Internet não tem um problema, o que a gente... tem que acontecer agora é torná-la mais segura sem invadir a privacidade, sem tocar na privacidade. A Internet é um sucesso, dadas as transformações digitais que ela vem sustentando hoje, não é? Todo mundo agora embarcando cada vez mais na Internet. E eu acredito agora que os profissionais estão migrando para torná-la mais segura.

SR. ANTONIO MARCOS MOREIRAS: Muito obrigado, Zamai.

Eu gostaria agora de pedir que a Vanessa Copetti Cravo, da Anatel, fizesse as suas considerações finais.

SRA. VANESSA COPETTI CRAVO: Obrigada.

SR. ANTONIO MARCOS MOREIRAS: Não tem nenhuma pergunta surpresa para você, Vanessa, aqui não tem.

SRA. VANESSA COPETTI CRAVO: Ah, que sorte a minha.

SR. ANTONIO MARCOS MOREIRAS: Não sobrou nenhuma. Exatamente.

[risos]

SRA. VANESSA COPETTI CRAVO: Fui beneficiada, então. Em primeiro lugar, então, agradecer novamente ao NIC por esse excelente convite, uma ótima oportunidade para a Anatel efetivamente mostrar o que tem feito nesse sentido, e apenas ressaltar que segurança é uma agenda prioritária da Anatel, e nós estamos empenhados em fomentar a construção de uma cultura de segurança cibernética no setor, e assim, então, dar a nossa contribuição para a segurança na Internet. E, nesse sentido, e também seguindo a linha do Moreiras antes, eu também vou fazer um jabá, mas é um jabá de certa forma coletivo, porque é uma iniciativa que tem assinatura coletiva, e eu convido a todos a acessarem, então, o Fique Esperto, fe.seg.br, com várias dicas de segurança nessa linha tão importante de conscientização dos usuários, inclusive com os vídeos do Cidadão na Rede, e também convidar a todos a acessarem o portal da Anatel, que está no gov.br/anatel, e em assuntos, além do 5G e de Celular Legal, por exemplo, vocês vão encontrar uma página destinada à segurança cibernética. Agradeço mais uma vez. Obrigada.

SR. ANTONIO MARCOS MOREIRAS: Nós é que agradecemos, Vanessa, a sua participação pessoal e a participação da Anatel aqui na nossa live.

E eu gostaria de convidar a Cristine também para as considerações finais. Também não tem perguntas surpresas para você, Cristine.

SRA. CRISTINE HOEPERS: Ah, nós somos privilegiadas, que bom. Eu queria comentar... assim, fazer as minhas considerações finais até reforçando algumas coisas que foram ditas agora, na última rodada, não é? Eu queria reforçar aquilo que o Parajo colocou, olha, bloquear coisas não é segurança. A gente vê... inclusive, hoje em dia a gente tem dificuldade de às vezes fazer o diagnóstico de problemas e de problemas de segurança pelo excesso de filtros, excesso de bloqueios. E lembrar que hoje, por exemplo, os ataques que estão comprometendo... não é, o pessoal falou muito no chat aqui, aqueles ataques comprometendo os roteadores de banda larga, lá o modem do provedor, eles estão vindo do *browser* do usuário, uma página invadida, é tudo misto, vem via Phishing, ataca a rede interna. Então, assim, bloquear não resolve os problemas. Não esperem uma lei, não é? Foquem no básico, foquem mesmo em coisas simples, e, sim, é muito mais interessante falar de tecnologias avançadas e querer que venha uma inteligência artificial mágica, mas o que a gente precisa é instalar *patches*, é colocar senhas mais fortes, é fazer segundo fator de autenticação, não é, eu acho que é focar no básico.

Queria muito reforçar o que o Zamai colocou, os melhores profissionais de segurança são aqueles que vêm de redes, porque a gente vê uma dificuldade grande do pessoal, às vezes, que vai direto para a segurança de interpretar Logs, de interpretar o que está acontecendo porque falta o conhecimento de como funciona, falta o conhecimento de [ininteligível], falta conhecimento de como funciona roteamento. Peguem uma base boa de redes antes e depois vão aí para a área de segurança, que sim, está precisando de gente, mas você precisa entender Internet primeiro, não é?

E eu acho que é na linha dos jabás, e até respondendo uma pergunta que o pessoal botou, "ah, a gente precisava de materiais para explicar LGPD para o cidadão", a gente tem na cartilha.cert.br os dois últimos materiais que foram lançados, são fascículos, um de proteção de dados e um de vazamento de dados. Eles foram feitos em colaboração com a ANPD. Então, a gente tenta em um falar o que fazer para proteger os seus dados, no outro o que fazer se tiver vazamento, e tem lá como entrar em contato, quais são os seus direitos. Ajudem a gente a divulgar esse material, porque a gente aqui, os nossos materiais, o Cidadão na Rede, o Fique Esperto... A gente tem lá no internetsegura.br material para crianças e para pais, porque muitas vezes os pais são os que estão gerando problemas aí para as crianças, não é? Ajudem a gente a divulgar. A gente está fazendo esse material gratuito, mas a gente precisa do boca a boca, precisa do efeito aí. E queria agradecer demais essa live. Aprendi muito, foi muito legal, e obrigada a todos aí.

SR. EDUARDO BARASAL MORALES: Nós que agradecemos aí a todos os painelistas. Realmente foi muito interessante tudo o que vocês explanaram para a gente hoje.

Bom, para a gente finalizar, eu gostaria de pedir aí, pessoal, para vocês preencherem o nosso formulário de avaliação. Então, o pessoal está colocando agora um QR Code aí na tela, está colocando um link no chat, que é para você dar uma nota de um até dez sobre a nossa live e também, se você quiser escrever um comentário, o que você gostaria de ouvir nas próximas lives, para deixar um tema, uma sugestão para a gente, o que a gente pode melhorar, fica à vontade, tá? Então, são duas perguntinhas básicas, pessoal, e isso vai nos ajudar bastante a melhorar o conteúdo do Intra Rede, tá?

Bom, queria deixar também avisos do nosso podcast Camada8. Então, semana que vem deve sair um novo episódio sobre o Camada8 lá. Então, acompanhem o nosso podcast aí na sua plataforma preferida, nos ajude a divulgar, tanto Intra Rede quanto Camada8. A gente gera todos esses conteúdos para você se especializar, para você repassar esse conhecimento para outras pessoas, tá? Por quê? Porque todo mundo tendo um maior nível de conhecimento, melhora a Internet para todos, a gente vai melhorar o nosso trabalho, o nosso serviço.

Temos também ali o curso IPv6 EAD. Então, quem quiser, pode se inscrever no curso IPv6 EAD, ele é aberto a todos, ele é gratuito, e você faz quando você tiver o seu tempo. Já o curso BCOP, a gente está com as inscrições abertas, tanto da turma 15 quanto da turma 16. A turma 15 se encerra hoje as inscrições. Então, tem que se inscrever. Depois, a gente vai fazer uma moderação da turma, tá, e aí aqueles selecionados vão participar. Então, é uma aula síncrona, diferente do curso IPv6, que a gente trabalha com uma aula assíncrona. Então, curso BCOP, que a gente fala de melhores práticas para sistemas autônomos, para provedores de Internet, provedores de conteúdo, administradores de rede, então quem quiser pode se inscrever, o pessoal está colocando o link aí no chat.

O próximo Intra Rede, ele vai acontecer em outubro, tá? A gente vai acabar pulando o mês de setembro, porque a gente tem um outro projeto, que é a Semana de Capacitação. Então, no dia 27 de outubro a gente volta com o Intra Rede falando sobre melhores práticas operacionais aí para o seu provedor, como você pode aprimorar a eficiência e a gestão do seu provedor, tá? Então, quem quiser, marca já aí no 27 de outubro, tá? A Semana de Capacitação, pessoal, ela acontece em setembro. Então, quem quiser... Eu vou pedir para o pessoal colocar o link aí no chat da Semana de Capacitação. A gente já está com todos os tutoriais lá, já dá para você se inscrever, tá? Tem a feira virtual também, pessoal, pode se inscrever lá na feira virtual. Lembra que aqueles bonequinhos é um espaço para fazer *networking*. Então, é uma oportunidade aí já de vocês continuarem se

especializando. Então, se inscrevam também na Semana de Capacitação, que acontece aí de 27 de setembro até 1º de outubro, tá? Então, são todos os dias com um tutorial diferente para você aprender colocando a mão na massa, tá?

Bom, vamos para o resultado dos sorteios aí, que o pessoal está muito interessado, não é? Sobre aquele kit do NIC, o sorteado foi o Luciano Alves de Siqueira. Então, é aquele kit de prêmios do NIC junto com alguns patrocinadores dessa live, que são vários prêmios lá, que o Moreiras até mostrou a foto. Então, é o Luciano Alves de Siqueira. Então, a gente vai entrar em contato com você depois. Do Netfinders Brasil, que era uma vaga do curso BGP e MPLS Avançado em Huawei em modo agravado, aí o sorteado foi o André. Ele só colocou o primeiro nome, André, e Netfinders Brasil vai entrar em contato com você. Sobre o sorteio da Globo, que é um voucher da Globoplay com acesso grátis ali por dois meses, quem ganhou foi o Jeferson Mira. Então, a Globo vai entrar em contato com você, Jeferson. E, por último, o último sorteio, que é o da GlobeNet, que é o fone de ouvido sem fio, quem ganhou foi o Bernardo Silva. Então, a GlobeNet vai entrar em contato com você, Bernardo. Esses são resultados dos sorteios que a gente teve aqui na live de hoje, tá? Espero que vocês continuem acompanhando o nosso Intra Rede, a gente vai ter outros sorteios, na Semana de Capacitação vão ter outros sorteios, então, quem quiser, pode acompanhar.

Para aqueles que querem o certificado dessa live, lembrando, as inscrições vão até às 14h, e tem que clicar no link enviado no e-mail. Se não clicar nesse período, não vai ganhar o certificado, é para aqueles que estão assistindo ao vivo, tá?

Gostaria de agradecer os patrocinadores, que é Juni Link IP & Cloud Network by GIOVANELI Consultoria, WZTECH Networks, ICANN, Netfinders Brasil, Novatec Editora, Eletronet, GlobeNet Telecom, Mundivox, 4Linux, Solintel, Cisco e Logicalis, 4Bios IT Academy, Globo, Netflix, FiberX e Huawei, e o apoio de mídia da revista RTI e Infra News Telecom, tá?

Então, para a gente terminar, como já foi falado bastante aí do projeto, eu vou chamar agora o videozinho do Cidadão na Rede. Então, pode tocar o videozinho.

[exibição de vídeo]

SR. ANTONIO MARCOS MOREIRAS: Pessoal, então, vocês viram mais um vídeo aí do Cidadão da Rede, e eu reforço: esse vídeo aí vocês conseguem disponibilizar ele nos seus próprios sites, nas suas redes sociais, vocês conseguem, inclusive, serem apoiadores do projeto e customizar esses vídeos com o logotipo da sua empresa. E nós estamos chegando ao final, ainda assim temos 380, mais de 380

pessoas, 390 pessoas assistindo ao vivo pelo Youtube, e agora eu não sei nas outras plataformas. Isso é bastante gente.

Eu quero dar só o último recado aqui, que não tem a ver com a live, mas eu sei que muitos de vocês que estão assistindo são técnicos aí de provedores e de outros sistemas autônomos, muita gente é participante do PTT de São Paulo. Então, vocês viram que hoje de manhã houve uma manutenção no portal do participante do PTT, no meu.ix.br. Nós fizemos modificações importantes lá. Nós mudamos... nós tornamos os links para você abrir chamados mais claros, o processo um pouquinho mais claro, e tem um novo módulo lá, que é um módulo de informações cadastrais, e nesse módulo agora você consegue atualizar informações que antes eram pedidas só no processo de inscrição, no processo de adesão ao PTT, e você tinha que abrir chamado para a gente atualizar, por exemplo, os contatos de NOC, os contatos de Peering, e algumas outras informações, que antes você tinha que abrir um chamado para que a nossa equipe atualizasse. Agora, você pode conferir isso e atualizar. Logo mais, quem é do PTT deve receber um e-mail explicando tudo isso, esse e-mail ainda não foi disparado, mas quem estiver aqui já pode entrar lá no meu.ix.br e dar uma olhada, dar uma olhada nesse módulo de informações cadastrais, conferir os dados que estão lá e manter os dados sempre atualizados. Tem dados lá que são públicos, tem dados que são disponibilizados no portal para os outros participantes e tem dados que a gente pede porque a gente precisa ter algum conhecimento sobre a rede de vocês para a gente melhor direcionar os nossos esforços, os nossos investimentos no IX.br. Então, tem um questionário lá com alguns dados que a gente pede, e são tratados sempre de forma confidencial. Está tudo muito bem especificado lá, temos a Política de Privacidade também lá disponível no site. Então, ficou esse recado aí, que está fora da live, mas está dentro do interesse do nosso público aqui, do público que nos acompanha sempre.

Volto a agradecer a todos os painelistas. Não vou citar nominalmente, mas muito obrigado a todos, muito obrigado a todos os nossos patrocinadores também, que tornam isso tudo viável, principalmente a questão dos sorteios, enfim, e gostaria de agradecer também a toda a equipe interna que nos apoiou para que essa live se realizasse, a própria... a nossa equipe do Ceptro, a equipe de comunicação, a equipe técnica que cuidou da transmissão. Muito obrigado a todos, e encerramos essa live agora. Obrigado.