SR. EDUARDO BARASAL MORALES: Bom dia, pessoal. Sejam todos bem-vindos aí a mais uma live Intra Rede que a gente tenta trazer aí as principais discussões no mundo das redes. Bom, na live de hoje a gente vai falar sobre como se prevenir e atuar durante um incidente de segurança. Mas antes de chamar nossos especialistas, gostaria de agradecer nossos patrocinadores, que é a Dattas Link IP, Servidores e Datacenter, FiberX, Globo, Icann, Netflix, 4Linux, Solintel/VLSM, Cisco e Super Conhecimento. Temos também o apoio de mídia da Revista RTI, Infra News Telecom e Editora Novatec. Lembrando, para quem quiser o certificado de participação dessa live, precisa se inscrever no link que está sendo colocado agora no chat. Se inscreve lá e fica atento ao e-mail, porque tem que clicar lá no link de confirmação. Então até 14h você tem como ganhar ali o certificado de participação dessa live. Então se inscreve no link colocado no chat e depois fica atento ao e-mail. Hoje também vamos ter sorteios, tá, pessoal? Então quem quiser, pode participar do sorteio do kit NIC, junto com os patrocinadores, que é uma camisa polo da Semana de Capacitação do NIC.br, uma lapiseira da Semana de Capacitação do NIC.br, um kit de adesivos do NIC.br, uma caneca da Icann, um kit Cisco de carregadores de celular, um kit Cisco de miniferramentas, uma senha de acesso da Super Conhecimento, válida por um ano, um livro Vida de Programador Volume 0 e um livro Vida de Programador Volume 1 da Editora Novatec. Tá? Esse é o mesmo link que você participa do certificado, para você ganhar o certificado. Então quem se inscrever para ganhar o certificado está participando do kit NIC. Teremos também alguns kits extras, que vão ser ali compostos por uma senha de acesso da Super Conhecimento, válido por um ano. E também ali o cupom de 25% de desconto na inscrição do curso telepresencial de segurança de redes da Solintel/VLSM, tá? Temos também um sorteio diferente, que agora um novo link de inscrição, que é da Globo, um voucher grátis de dois meses para o Globoplay, válido somente para novos assinantes. É um novo link, quem quiser, pode se inscrever. E temos também o sorteio da 4Linux, um curso da 4Linux a escolha do ganhador. É um novo link que está sendo colocado no chat, quem quiser, pode se inscrever em todos esses sorteios que a gente depois, no final da live, vai falar o ganhador.

Bom, como já é de praxe, eu gostaria de chamar aí o vídeozinho do Cidadão na Rede, que explica um pouquinho aí como ser um bom cidadão na Internet. Lembrando que as empresas que quiserem podem baixar esses vídeos e colocar o logo delas dentro do vídeo. Então, vamos tocar o vídeo.

[exibição de vídeo]

SR. ANTONIO MARCOS MOREIRAS: Agora sim. Bom dia a todos, bom dia a todas, que estão aqui acompanhando o nosso evento, mais um Intra Rede. Estou vendo que temos aí 430 pessoas assistindo agora, bastante gente já. Mas eu sei que tem aquele pessoal que acorda mais tarde ou está distraído com o serviço, chegou até mais cedo no serviço para conseguir adiantar todas as tarefas, para poder ter o tempinho aqui para ver os nossos especialistas de segurança. Enfim, é aquele momento que a gente dá aquela pequena enroladinha para... até para dar tempo de vocês chamarem os colegas de vocês, colocarem o link lá naquele grupo de WhatsApp do trabalho, grupo de WhatsApp, de Telegram, de Facebook, de sei lá o que vocês participam aí com os colegas de profissão, e os colegas de faculdade, os colegas de curso técnico, e chamar todo mundo para assistir ao vivo aqui a nossa live. Isso, a live, ela fica gravada no YouTube. O mesmo link que vocês estão assistindo agora, vocês podem compartilhar com os colegas, tal, ou mesmo vocês, se quiserem voltar e rever o conteúdo com mais calma depois, eu mesmo faço isso sempre. O link é o mesmo. Imediatamente depois que termina a live, ele já fica disponível, ele já está disponível. É só entrar e assistir de novo e está tudo certo. Então a live fica gravada e disponível no YouTube. Os palestrantes que usarem PowerPoints, usarem apresentações, eles, alguns deles já nos mandaram. Daqui a pouquinho elas vão estar disponíveis lá no site: intrarede.nic.br, elas vão sendo colocadas durante o próprio evento, vão dando o *refresh* na página e vão conseguir fazer o download dos slides para dar uma olhada, para em alguns casos até acompanhar junto. Vocês podem interagir com a gente no chat. Muita gente dando bom dia agora. Até convido vocês aí para fazerem uso do chat agora, dizerem da onde vocês são, de que provedor, em que provedor vocês trabalham, que empresa vocês trabalham, que faculdade que vocês estudam, de que estado, de que cidade vocês estão falando aí. Nos digam no chat para a gente ter ideia da onde a gente está chegando. Tem alguém de fora do Brasil? Às vezes tem gente de Portugal, de Angola. Bastante gente. Brasília, Vila Velha, Espírito Santo, Nilópolis, Belém do Pará, Recife, Caieiras, São Paulo, Nova Iguaçu, Timbó, BH, Fortaleza, Presidente Prudente, Aracaju, Manaus... tem gente do Tribunal Regional do Trabalho, tem gente... Nossa, não estou conseguindo nem ler aqui. Muita gente do Brasil inteiro. É muito legal. A gente fica bastante satisfeito, bastante feliz com a abrangência que essa live está tendo, né? É uma responsabilidade, hein, pessoal? Os palestrantes aqui. A gente convidou palestrantes excelentes, de primeiro nível aqui.

Bom, vocês podem interagir com a gente no chat, durante a live inteira, mesmo quando os palestrantes estiverem apresentando. Como vai funcionar? Os palestrantes vão ter 15 a 20 minutos de apresentação cada um deles. Nesse momento, eles não vão responder perguntas. Eles trouxeram uma apresentação pronta. Eles provavelmente não vão

conseguir interagir com vocês enquanto eles estão fazendo essa apresentação. Nesse momento, nossa equipe está anotando todas as perguntas lá do chat. Quando acabarem, todos os palestrantes acabarem de fazer a apresentação inicial, a gente vai começar a fazer as perguntas. Vamos selecionar perguntas que foram feitas durante o chat e vamos começar a interagir com os palestrantes, colocando essas perguntas para eles. Nem sempre dá tempo da gente colocar todas as perguntas, fazer todas as perguntas. A gente tem que ter um limite de tempo aqui para a live. Os palestrantes, eles foram convidados a responder as principais perguntas que ficarem de fora dessa interação nos comentários do YouTube. Se vocês entrarem, por exemplo, no vídeo da live anterior, vocês vão ver que os palestrantes fizeram isso. E a gente achou muito legal. Alguns palestrantes fizeram até por conta própria, né? Foi ideia de um deles, para ser bem específico aqui, dar o crédito, foi ideia do Henry, da Unicamp. E a gente achou sensacional. E a gente começou a convidar os palestrantes a fazerem isso. Então alguns deles vão fazer isso. Convido vocês, então, depois da live, a entrarem de novo no YouTube, darem uma olhada lá, senão no vídeo inteiro, darem uma olhada justamente nessa parte de comentários porque vão ter algumas respostas lá, algumas coisas interessantes. A gente falou, às vezes, alguém faz uma pergunta aqui que a gente mesmo não percebe a relevância, mas depois o palestrante olha e fala: "Nossa, que ponto importante. Devia ter abordado isso na minha palestra, ficou de fora, vou aqui fazer um comentário, vou aqui responder essa dúvida". Então pode ser interessante dar uma olhada geral. Queria pedir para vocês deixarem o like. Deixarem o joinha aí no YouTube. Isso é importante para a gente. Isso faz com que a plataforma, faz com que o YouTube, faz com que o Facebook, para quem está assistindo via Facebook, distribua organicamente, mostre o vídeo organicamente, de forma natural, sem a gente ter que pagar impulsionamento para mais gente.

Então, por enquanto aqui, não chegamos no conteúdo ainda, já vou passar a palavra para a Lucimara, mas o conteúdo a gente tem certeza, pelo nível dos palestrantes que a gente convidou, que vai ser excelente. E a gente quer fazer esse conteúdo chegar no maior número de pessoas, no maior número de técnicos, no maior número de redes, de provedores, de administradores de rede aí que for possível. E o like de vocês ajuda bastante nisso. Então a gente tem 577 pessoas agora assistindo ao vivo, temos 317 likes. Eu quero pedir o voto de confiança para vocês. Deixa o like para não esquecer depois. Cara, se você não gostar do conteúdo, aí você vai lá e tira o like. Tenho certeza que se você não gostar, você vai lembrar de ir lá e tirar o like. Mas se você gostar, talvez você esqueça de ir lá e deixar o like no final. Então dá o voto de confiança aí para a gente. Quem acompanhou as lives anteriores pode dizer se foram ou não foram boas aí no chat. Aliás, gente, tem alguém pela primeira vez aqui? Tem alguém aqui que nunca

acompanhou um Intra Rede nosso e chegou aqui na live pela primeira vez? Diga aí no chat para a gente saber.

Bom, vamos lá, gente. Sem mais delongas, já enrolei bastante. Já temos aqui quase 600 pessoas assistindo. Vamos começar com conteúdo. Nossa, tem bastante gente pela primeira vez. Vamos começar agora com o conteúdo de verdade. Eu não vou apresentar, a gente não vai apresentar palestrante por palestrante, dar o currículo, eu vou falar o nome, o Eduardo também, a gente vai falar a instituição, da onde o participante... da onde o palestrante vem. O palestrante pode se apresentar melhor, com mais detalhes. A gente também tem os minicurrículos dos palestrantes lá no site do Intra Rede. Então quem tiver curiosidade, dá uma olhada lá. E vamos seguir assim. A nossa primeira palestrante é da casa, é do NIC.br. Ela trabalha no CERT.br, é a Lucimara. Lucimara, então, você pode assumir aqui o microfone e seguir?

SRA. LUCIMARA DESIDERÁ: Estão me ouvindo? Pessoal está me ouvindo? Vou fazer aquele momento de tensão que é compartilhar os slides. Só um minutinho, vamos voltar aqui para a apresentação. *Share screen*. Pessoal está vendo aí a minha apresentação? Beleza. Deixa só eu abaixar. Então vamos lá. Vamos cronometrar aqui para não perder o tempo. Aí, então, bom dia, pessoal. Muito obrigada ao convite da organização para participar. Como muitos já sabem, meu nome é Lucimara, eu sou... Ops, vamos lá. Por que você não está indo? Eu sou analista de segurança no CERT.br e hoje vou começar falando um pouquinho sobre gestão de incidentes, né? Vou dar uma pincelada aí em algumas coisas que a gente tem visto, a razão de alguns incidentes que estão ocorrendo mais recentemente e basicamente depois eu vou falar sobre o processo de gestão de incidentes. Eu não vou entrar em detalhes de resolver incidentes. Eu vou deixar isso para os próximos palestrantes, né? A experiência deles. E agora eu vou falar um pouquinho mais sobre a nossa... o que a gente tem visto e a parte de gestão de incidentes.

Então, o que a gente tem visto mais recentemente? Aquele que tem sido reportado, aquilo que a gente tem observado com alguma frequência nos últimos anos? Aí também com os feeds, coisas que a gente recebe, as nossas análises, né? A gente tem visto que os principais ataques que estão acontecendo recentemente, a causa, o que eles mais buscam como mecanismo de entrada e causas de intrusões, vazamentos e coisas assim, tem a ver... está relacionado com senha, com exploração, descobrir senha que, ou está fraca, ou vazou e continua sendo utilizada. E isso afeta muitos serviços, né? Principalmente afetando serviços em cloud, entrada em VPN, que acaba dando acesso à organização, a porta de entrada. E outro mecanismo que vemos bastante também é exploração de vulnerabilidades conhecidas. Vulnerabilidades que já têm patches

disponíveis há algum tempo, né? Então a gente tem visto que mais de 80% dos incidentes poderiam ser evitados se patches fossem aplicados e se todos os serviços tivessem um duplo fator de autenticação, múltiplo fator de autenticação. Então se a gente puder fazer aí um apelo para as organizações ou se a gente pudesse dar um conselho para as empresas, eu vou aqui fazer minhas as palavras da Katie Moussouris, que é pesquisadora da área de segurança internacional, *multifactor everything*. A primeira coisa que eu recomendo para todos, para diminuir aí os incidentes que a gente tem visto bastante nos últimos tempos é *multifactor*. Ah, Lucimara, quer dizer, então, que se eu aplicar patch e botar *multifactor* eu resolvi todos os problemas? Negativo. Absolutamente não. Não existe segurança 100%. E mesmo os sistemas bastante seguros e organizações que têm tradição em trabalhar com segurança, como a gente vê lá, RSA, DOD, o pessoal do governo da Holanda, tiveram grandes incidentes e precisaram lidar com o incidente, né? Então falar de incidentes, a gente tem que começar falando de risco, né? Porque, na verdade, não existe segurança 100%. Sempre vai existir um risco. Risco é uma intercessão de coisas, né? Ele está relacionado com os ativos, né? Com sistemas e dados e as pessoas. Esses sistemas, e esses dados, e essas pessoas, eles têm vulnerabilidades. Isso começa por projetos sem prioridade de segurança, defeitos de software, falhas de configuração, uso inadequado e aí entra também até questão do *insider*, né? As pessoas que acabam se aproveitando dos seus privilégios, do seu uso para fazer acesso indevido. E outras fraquezas vindas da própria complexidade dos sistemas, as integrações, as pessoas não conhecem todos os meandros e acabam deixando falhas de configuração. Outra coisa que afeta o risco são as ameaças, né? Então isso a gente tem criminosos querendo ganhar dinheiro, a gente tem espionagem industrial, tem os governos, a gente tem visto isso muito, né? Nos últimos anos aí, vê a Rússia brigando com Estados Unidos, invadindo, e uma série de coisas assim. Então os governos têm um papel bastante grande, uma ameaça bastante presente nos dias atuais. E a gente não pode esquecer daqueles vândalos, né? Aquele que quer pichar a página, que quer causar tumulto, né? Então isso tudo junto a gente vai ter lá, então, os riscos. Quais são os riscos que a gente tem na nossa operação, né? Indisponibilidade de serviço, a gente vai ter... pode ter perda de privacidade, furto e destruição de dados, e tudo isso acarreta aí, trazem perdas financeiras, danos à imagem da empresa e, eventualmente, até a perda da confiança na tecnologia. Então para a gente trabalhar com o risco, o que a gente pode fazer com o risco? A gente pode aceitar, simplesmente não fazer nada. A gente pode transferir isso, a gente faz isso no nosso dia a dia, por exemplo, quando a gente contrata um seguro, mas nem tudo a gente consegue contratar um seguro. E a gente pode... não consegue, normalmente, eliminar risco. Único jeito de eliminar risco seria eliminar algum dos vértices

que a gente imagina que é muito difícil. Não tem como tirar nossos ativos da rede, a gente não tem como eliminar algumas ameaças, o que a gente consegue fazer é mitigar. Mitigar o risco é opção mais palpável e mais real da gente se fazer. E aí, então, mitigar risco significa o quê? Reduzir a probabilidade da gente ter um incidente e minimizar também, diminuir qual é o impacto daquilo. Então a gestão de incidentes nos ajuda a detectar precocemente e reduzir os danos.

Então quando a gente fala: esses incidentes vão ocorrer? Vão, não tem segurança 100%, a gente precisa pensar em resiliência. a gente precisa continuar funcionando mesmo na presença de falhas e ataques. E o que é primordial para a gente pensar, então? A gente precisa ter aí... só abaixar aqui um pouquinho. A gente precisa ter políticas, ter estratégias, ter profissionais treinados para executar essas políticas, né? A gente precisa ter pessoas conscientizadas sobre os riscos e o papel delas, no contexto, nos processos da empresa. E a gente precisa tenho ter tratamento de incidentes, né? Espaço aí para implementação dos grupos de resposta a incidente de tratamento, tratamento de incidentes, normalmente chamados CSIRTs, né? Que é o Computer Security Incident Response Team, que a gente trabalha aí com acrônimo CSIRT. Tá?

Então o que é gestão de incidentes? Gestão de incidente é um conjunto de processos, né? Começa lá com a alta gestão da organização se conscientizando, compreendendo a importância e apoiar aí o desenvolvimento desse conjunto de processos. Porque a gestão de incidentes não é instalar uma aplicação, uma ferramenta para gerar ticket de chamado. Gestão de incidentes vai muito além disso. Ela compreende aí o desenvolvimento de um plano de ação, um conjunto de políticas, de processos, que serão consistentes, que sejam repetíveis e que vão acabar envolvendo diferentes áreas da organização no tratamento de incidente. Por que eu falo repetíveis? Por que falo de definir os processos? Porque pensar em tratar incidente na base do improviso vai ser problema, né? Muito provavelmente você não vai conseguir dar a resposta adequada no tempo necessário, e quanto mais tempo você leva para dar uma resposta, para tratar, você... para descobrir, fazer tratamento, você vai ter cada vez mais impactos e prejuízos, danos que vão ser causados. É preciso... pensamento tenho de incidente, é um processo contínuo, de identificar, prevenir, mitigar e responder. Nem sempre essas funções todas são executadas dentro de única entidade na organização. Pode passar por várias entidades da organização, e por isso que é preciso a gente disseminar informações de maneira adequada para que o incidente possa ser resolvido de maneira adequada, né? Então gestão de incidente também está integrado, tem a ver com estar preparado para tratar o incidente, mas ela precisa estar integrada também com a parte de proteção da empresa, né? Então a gente precisa, por exemplo, de

um processo de tratamento de incidente lá em uma resposta: "Ah, eu preciso mitigar, criar uma regra de firewall". Então a gente precisa estar integrado aqui com todos os processos, com as partes e organizações que implementam, por exemplo, mecanismos de proteção de rede, né? Então gestão de incidente significa estar integrado com toda parte da proteção e estar preparado para lidar com incidentes. Esse [ininteligível] aqui, que é o *detect*, triagem e responde, isso é basicamente tratamento de incidente, todo o resto junto, a preparação de políticas e esse mecanismo contínuo de feedback para você melhorar o seu processo, para você evitar eventualmente que um incidente aconteça e proteger a organização, isso é um processo contínuo, tá?

E, eventualmente, a gente tem aí diferentes fluxos de resposta a incidentes. Então uma empresa pode tratar diferentes tipos de incidente e eventualmente também tem diferentes respostas. Você pode ter uma resposta, que ela é técnica, e você pode ter uma parte da resposta que é gerencial. Então quando a gente está falando, principalmente aqui eu trouxe como exemplo a LGPD, que fala em ter que notificar incidente para a autoridade nacional em caso de um risco ou dano relevante aos titulares. Então a gente tem aqui o processo de tratamento de incidentes lá em uma certa parte dele para a frente a gente precisa entender o escopo, a natureza dele e avaliar se há necessidade de uma resposta gerencial, de identificar se é necessário uma resposta legal. E aí a gente tem que se perguntar: Isso foi um crime? Preciso acionar as operadoras na Justiça? Isso teve uma quebra de contrato? Eu preciso acionar o meu jurídico para eventualmente, sei lá, tive problema... vai impactar uma SLA de um contrato meu. E outro caso é: envolve dados pessoais? Ah, sim, então talvez vou precisar acionar o meu jurídico para que se faça relatório e isso seja encaminhado à ANPD no caso de se tiver um risco ou dano relevante para titulares e organizações. Então neste caso aqui a ANPD, ela é um stakeholder do processo. Então se vocês olharem, aqui a gente tem um fluxo de resposta de incidente, como eu disse: tem a resposta técnica e a resposta gerencial da qual a resposta legal é parte. Então normalmente, um CSIRT, por exemplo, não vai fazer uma resposta legal, uma resposta de gestão. Ele interage junto, ele é o ponto de contato e vai levar isso para equipe gerencial e aí envolver partes necessárias para que os stakeholders sejam notificados e comunicados. Uma coisa que vou frisar é que a parte de comunicação é muito importante na parte de resposta a incidentes, porque se a informação não flui de maneira adequada a gente vai ter problema.

Bom, e gestão de incidentes, ela não é isolada. Gestão de incidentes, ela está aí permeada em diferentes frameworks, e aqui cito um dos frameworks que tem sido bastante utilizados na nossa área, tem sido recomendado [ininteligível] segurança cibernética do Brasil e

várias instituições, que é o framework do Nist. Então, se alguém quer entender um pouco mais do contexto de segurança cibernética e de como isso... como fazer a gestão de segurança, a gente vai entender, olhar aqui. E é interessante observar que a grande maioria das partes desse framework tem a ver com gestão de incidente. Então começa lá com identificação dos riscos do negócio e da tecnologia, e aí você define, então, os mecanismos de proteção da sua infraestrutura e toda essa parte tem a ver com gestão de incidente, que é detectar, responder e fazer a recuperação do incidente.

Para quem está pensando em montar um grupo de resposta a incidentes, eu sugiro dar uma olhada no framework de serviços do First, então esse framework foi desenvolvido pela comunidade de CSIRTs, inclusive, uma das pessoas do CERT.br participou da criação desse documento. Ele é hoje considerado um padrão para a área, né? E aí vocês podem ver lá quais são todas as áreas de serviço que um grupo de resposta a incidentes pode ofertar. Não necessariamente você precisa oferecer todas, você pode escolher algumas áreas em que você quer atuar. E esse framework, ele traz, além dessas várias áreas de serviços, ele traz cada uma das funções executadas e quais são as saídas e os inputs de informação que fazem parte do processo... dessas funções, entre elas aqui, a parte de gestão de incidentes, né? E entre outras que você... cada organização é que vai determinar o quanto que ela pode... o que ela quer fazer de serviço.

Bom, eu já sabia que não ia dar tempo de falar muito mais coisa. Então vou colocar algumas referências adicionais para vocês virem depois no material. O trabalho do CERT.br, o que a gente tem feito na área aí, né? A gente está há 25 anos trabalhando para aumentar a capacidade nacional de tratamento de incidentes. Nosso foco é ajudar profissionais, ter profissionais preparados e aproximar os grupos de CSIRT para que eles possam interagir. Porque o fato é: não existe resposta a incidentes isolada, a gente depende de outros grupos de respostas a incidentes para conseguir fazer o nosso trabalho. Normalmente, o incidente acaba envolvendo diferentes organizações e você precisam ter contatos nas diferentes organizações. Para isso, a gente faz, a gente tem a lista de CSIRTs brasileiros que podem servir de consulta. Tem fórum que a gente faz. E a gente tem os nossos cursos de capacitação, que a gente está formando sempre gente em área de resposta a incidentes. Outra coisa interessante mencionar: gestão de incidentes, resposta a incidentes tem um código de ética. Então é superimportante se inteirar disso, entender o que faz parte, do ponto de vista ético no tratamento de incidentes. E a gente passa por desde questão do dever de confidencialidade, do dever de respeitar direitos humanos e uma série de outras coisas, recomendo dar uma olhadinha na parte do código de ética.

Por fim, quem quiser fazer um esforço extra, quiser entender, já existe o modelo de maturidade, já existe avaliação de maturidade na área de tratamento de incidentes e respostas a incidentes, e gestão como um todo, né? E aí tem o modelo do SIM3, quem quiser conhecer um pouquinho mais e eventualmente avaliar o seu nível de maturidade na área de tratamento de incidentes, eu deixo a ferramenta do SIM3 para avaliação. É isso, pessoal. Estou devolvendo aí o controle para a Mesa.

SR. EDUARDO BARASAL MORALES: Obrigado, Lucimara. Muito interessante tudo aí que você apresentou. Bom, queria avisar o pessoal que quem quiser pode mandar sua pergunta no chat. Tiver dúvida para a Lucimara, fique à vontade para mandar no chat do YouTube, que a gente está coletando todas as perguntas para depois fazer elas no ao vivo. Tudo bem? Não se acanhem.

Gostaria de chamar o próximo palestrante, o Alexandre Berto Nogueira, do CSIRT da Unicamp. Alexandre, fica à vontade. O palco é seu.

SR. ALEXANDRE BERTO NOGUEIRA: Bom dia, pessoal, bom dia a todos. Deixa EU só compartilhar minha tela. Um momento só. Bom dia, é uma honra estarmos aqui presente representando a Unicamp, estamos muito felizes de sermos convidados para estar mostrando um pouco da experiência que nós temos. E acredito que pode ser de muita valia para todos os provedores, todos que estejam assistindo nesse instante aqui. Bom, temos uma agenda e vamos procurar segui-la, mas com o tempo que nós temos... e eu já esqueci de cronometrar, mas vamos lá. A gente vai falar um pouco da Unicamp na apresentação, fazer uma apresentação rápida dela. As bases. A gente encara que para fazer uma prevenção eficaz de um incidente, baseado na nossa experiência, a gente separa em três bases, né? Nós vamos falar um pouco delas e vamos também dar uma ênfase no uso de flows na prevenção e na atuação em incidentes de segurança. Tá certo? Temos bastante, alguma experiência com uso de flows, tem sido um aliado muito interessante para o nosso dia a dia, para não dizer extremamente importante, e vamos fazer uma conclusão disso. Tudo certo, o áudio e a apresentação? Tudo certo? Ok?

A CSIRT da Unicamp, é um CSIRT, conforme a Lucimara até comentou, somos 1 CSIRT com 25 anos, foi criado em 1997, basicamente fazemos toda tratativa dos incidentes de segurança, todo o ciclo de vida. Temos alguns serviços que fomos agregando nesses 25 anos, como o uso de flows de rede, né? Começamos a introduzir na análise diária do nosso dia a dia. Fazemos também alguns testes preventivos com a finalidade de fazer detecção de possíveis brechas, vulnerabilidades, isso, tanto a nível de rede como a nível de interface web também, aplicações web. Também fazemos ministração de

palestras de conscientização, tanto a usuários finais como usuários técnicos. Acreditamos que seja muito importante, pois, como também a Lucimara falou, roubo de credenciais se tornou muito comum, roubo de credenciais ou tentar adivinhar parzinho, usuário e senha, ou tentar utilizar uma credencial válida para acessar serviços do dia a dia. Então também emitimos alguns certificados digitais com a parceria da Globalsign com a RNP. E também somos um CSIRT de coordenação. Essa expressão vai se tornar um pouco mais amigável para vocês quando a gente falar um pouco sobre o diagrama. A Unicamp é basicamente um provedor. Se a gente colocar Unicamp, nós, no centro de computação, nós, do CSIRT, seria como fosse a equipe de segurança, por exemplo, de uma Embratel, e você tem várias empresas conectadas ao seu *backbone*, e elas reportam a nós. Nós retransmitimos, nós repassamos o incidente, repassamos algum problema para cada órgão, núcleo, faculdade, instituto, centro de pesquisa que está conectado ao *backbone* da universidade, tá?

Uma frase ou três frases, como você preferir, que acredito que cabe muito no nosso dia a dia de trabalho. É o almirante William Halsey, ele criou essa frase no ambiente militar, mas podemos trazer tranquilamente para o nosso ambiente de segurança, tá certo? Que é essa: *"Hit hard, hit first, hit often".* E acredito que fala muito sobre o que é nós. O *hit hard*... você vê, qual é a nossa missão? Sempre procurar atingir o inimigo ou atingir o nosso objetivo de uma maneira precisa, de uma maneira contundente, né? Isso vai muito com a identidade de um CSIRT, [ininteligível] muito com a identidade de um grupo de segurança. Você precisa ter uma identidade, você precisa ter uma infraestrutura, você precisa ter um órgão que funcione e funcione adequadamente. O *hit first* é aquele nosso desejo que muitas vezes a gente não consegue, que é pegar o inimigo primeiro. Descobrir a vulnerabilidade primeiro, antes que uma pessoa maliciosa consiga fazer isso. Descobrir aquilo, uma brecha infringida ou um ataque primeiro antes que ele cause mais danos, tá certo? E *hit often*, que é a nossa eterna procura por brechas de segurança. Nós não podemos parar, não é uma coisa estática, ela é funcional e ela tem que ser diariamente no nosso dia a dia de trabalho.

Então, como falei a dois slides passados, a Unicamp se assemelha muito ao provedor. Esse é o *backbone* da universidade, como ela se conecta na Internet. E os institutos, núcleos, eles são descentralizados, ele tem sua própria área de TI e se conectam nesse *backbone*. Dessa forma, eu acredito que tudo que a gente faz no nosso ambiente pode ser de grande valia para todos que estão assistindo, pois, a gente meio que se assemelha a um provedor médio que podemos dar conectividade para provedores menores aí.

Bom, o que nós entendemos quando a gente fala de prevenção? De acordo com nossa experiência e o nosso dia a dia, a gente pode

separar prevenção em três bases. Primeira base seria identidade de um time. Ou seja, a Lucimara falou um pouco sobre isso, mas eu queria ressaltar alguns pontos, né? Não só da formação, não só de ter um controle e histórico de um chamado, processos definidos que se fala muito, mas acreditamos que você precisa ter canais de comunicação abertos. Ou seja, eles precisam ser funcionais, precisam ter uma rapidez, uma rapidez de você conseguir achar o contato daquele instituto, o contato daquele órgão e poder trocar as informações de forma ágil. E ele precisa ser funcional também, ou seja, precisa ser atualizado. A gente vê muito isso quando vai tentar fazer algum contato com o whois, não consegue porque não está atualizado. E a gente também pode perceber que na identidade do time é preciso ter uma permeabilidade organizacional. Nome difícil que eu coloquei, mas é exatamente isso. O CSIRT, ele precisa ter comunicação, não só comunicação, mas ele precisa andar, vamos colocar dessa forma, em toda... precisa ter pé em todos os órgãos da hierarquia. Ele não pode ser estanque. Ele não pode ser isolado, agir de forma isolada. Tem que ter liberdade de comunicação e de ação com qualquer nível, qualquer nível hierárquico. E um outro ponto que eu queria ressaltar seriam os indicadores. Você tem seu trabalho, você tem os seus chamados, você tem as suas vulnerabilidades [ininteligível] e tudo mais, mas você precisa colocar isso no papel. Você precisa ter isso para buscar o histórico: será que estou melhorando? Como eu estou? Como é a visão que eu estou tendo desse meu trabalho que eu estou fazendo? Uma outra base que identificamos como suma importância é que você tem que ter uma boa visão da sua infraestrutura. O que seria boa visão da sua infraestrutura? Não é só um diagrama, não é só um inventário de máquinas, também é mas também algo maior, como: qual o comportamento normal padrão da sua rede? Como que eu vou descobrir problemas, anomalias de tráfego, se eu não sei o comportamento padrão da minha rede? Então você precisa conhecer. Como você vai conhecer? Existem diversas ferramentas de monitoramento, de análises de tráfego, que podem te dar essa visão e podem te auxiliar em você descobrir o comportamento padrão da sua rede. Também é muito importante que você tenha uma infraestrutura de logs, de registro de logs, não só os logs de aplicação, mas logs de dispositivos, logs de todos os ativos da sua rede, concentrado em estruturas remotas e sincronizadas. Temos aí [ininteligível] que pode auxiliar a todos a manterem o registro de logs sincronizados. Não existe coisa pior do que tentar fazer uma análise de um incidente e todos os horários não se correlacionam. Você vai ficar rendido, você não vai conseguir fazer é nada. E também que nós vemos como de extrema importância para você ter uma visão da sua rede é você utilizar uma ferramenta que mostre o padrão da sua rede, o tráfego da sua rede, como flows. Os flows de rede podem te auxiliar, e você tem alguns sabores dos principais aí: Netflow, Sflow e IPfix. Não só

identidade, não só a visão mas também uma avaliação continuada. O que seria isso? Eu tenho a visão da sua rede, tenho um time forte, tinha um time bem construído, mas você não pode ficar parado. Você tem que ter um ferramental para fazer varreduras na sua rede, para procurar brechas. Até os [ininteligível] colocou uma frase que é muito interessante, que se você não faz frequentemente varreduras procurando vulnerabilidade na sua rede, você está fadado a ter um incidente de segurança, uma invasão. Então você... é necessário você fazer diversos tipos de varredura, tanto a nível de rede como a nível de web, ou outras mais que a gente puder incluir aí. Conscientização de usuários é um trabalho contínuo. Você não faz uma vez e para. Porque você tem novas ameaças, você tem novas pessoas chegando, algumas pessoas saindo, então você tem que ter conscientização frequente dos seus usuários. Isso tem que estar também bem parametrizado, com uma boa política, uma boa instrução normativa para te auxiliar nisso tudo. E investir em capacitação dos técnicos, isso é muito importante. Buscar a capacitação, ir atrás. Bater na porta da chefia e falar: Precisamos nos capacitar nisso. Lucimara inclusive até falou sobre as capacitações do Cert. Nós fizemos as capacitações do Cert, foram muito boas, para nos auxiliar a parte... tanto a parte de incidente como a parte do dia a dia de um CSIRT, né? Então consultem lá. E também uma expressão que está muito na moda, né? Threat Hunting. E isso, aliado com os flows, é uma brincadeirinha bem gostosa de fazer. Você tenta se antecipar a um problema na sua rede, procurar mesmo uma sarna para se coçar, ver se tem algo fugindo do padrão, ver se aquela ameaça está chegando em você, tá certo?

Mas vamos focar um pouco mais na visão de infraestrutura, principalmente na parte de flows de rede. Bom, flows de rede é um assunto que dá muita discussão e ninguém vai chegar no conceito próprio. Você pode chamar amigos para beber uma cerveja, mas não vai conseguir chegar a um conceito próprio. Eu sei que... trouxe algumas definições aí, não vou falar todas, depois vocês podem dar uma olhada, mas um *timeline* que é necessário, né? Começou tudo com o Netflow da Cisco, que foi implementando até a versão 8. Aí temos o Sflow, ou seja, a definição dele que veio em 2001, tá? Até chegar ao IPFIX em 2008. Mas, basicamente, como funciona? Flows é uma capacidade, é um protocolo que funciona dentro de cada ativo de rede, né? Então nós podemos ver um ativo de rede recebendo várias conexões, vários tráfegos passando por ele. Ele tem um mecanismo que ele seleciona um pacote, armazena as informações básicas desse pacote, não armazena o *payload* do pacote, e vai encapsulando isso num pacote sflow e envia para um coletor e a partir desse coletor pode fazer uma análise mais profunda mais a fundo [ininteligível].

Trouxe aqui, baseado nesse desenho os agentes e os *exports* que são ativos de rede, né? Temos um Netflow coletor ou um coletor de

sflow, que é geralmente uma ferramenta que vai armazenar seus flows, e o *front-end*, que vai te dar uma visão daquilo que você está analisando. Então trouxe para vocês aqui uma tabelinha, depois vocês vão ter a oportunidade de consultar, alguns agentes mais conhecidos aí de sflow, né? Então você tem Cisco, Aruba, tem Juniper, tem o Extreme, tá certo? O IPFIX, que é a padronização do Netflow, que nós temos as opções inclusive com o Mikrotik, e o Netflow versão 9, que também pode ser utilizado com Mikrotik. E os coletores e os *front-end*s, nós temos diversas também. Não coloquei todos. Tem alguns que você pode começar a brincar aí. Mas a Unicamp, eu vou utilizar slides em cima disso, ela trabalha especificamente com [ininteligível], e eu tenho que correr. Basicamente na experiência da Unicamp nós temos algumas possibilidades que nós podemos fazer com flows. Você pode criar relatórios de principais agentes que estão trafegando na sua rede, protocolos. No incidente de segurança que foi também nosso caso, a gente utilizou muito para fazer correlação, correlação de data e tráfego para dar um *timeline* nos nossos incidentes, que é muito importante. Pode auxiliar você na defesa contra os ataques DDoS, ou seja, serviços de TCP ou UDP que possam estar abertas aí. Você pode utilizar flows, fazer uma análise com fontes conhecidas de endereços maliciosos e aí você faz um relatório. Isso tudo por via scripts, né? E um script também nós utilizamos aqui, ou seja, quanto de IPv4 eu estou usando realmente na minha rede, tá certo? Não é só o que está baseado no seu /24 ou no seu /20, tal, mas como eu realmente estou utilizando. Será que estou utilizando todos os endereços? Através dos flows você tem mecanismos para saber isso, [ininteligível] que você pode fazer.

Dois exemplos rapidinho de como a gente pode utilizar o nfsen, que é um *front-end* do nf dump, que é um coletor de flows, para identificar um comportamento estranho na rede. Por exemplo, a gente está vendo uma telinha básica do nfsen, ele é bem antigo, não é tão moderno assim. A gente vê o pico de tráfego um pouco antes da meia-noite aí. A gente consegue, por exemplo, isolar esse pico, colocar algumas informações de opções e ter uma saída gráfica, tá? Eu só coloquei a partir de Asc(F), uma saída gráfica do que aquilo está nos causando. No caso foi um pico possivelmente um SSH, um [ininteligível] sendo rodado nesse momento aí, tá certo?

Também um fato interessante, queria ressaltar, que é a versatilidade. A gente falou do nfsen, que é um *front-end* gráfico, mas o nf dump é como se fosse um TCP dump dos flows. Você pode utilizar ele muito. Por exemplo, o CERT.br colocou uma informação, mandou um e-mail lá em 24 de fevereiro, se não me engano, sobre a gente cuidar da nossa infraestrutura para não estar sendo vetor de ataques DDoS contra a Rússia. Então o que nós fizemos? A gente pegou, fez um parseamento dos ASs da Ucrânia. Em uma ferramenta, por exemplo, [ininteligível], parseamos tudo, fizemos uma consulta e

deixamos essa consulta rolar. Basicamente a gente sabia previamente se a gente está tendo alto tráfego com destino à Ucrânia por causa dessa própria versatilidade do nfdump. Então isso é só um exemplo, você pode utilizar muitos outros para atuar na infraestrutura.

E quanto que isso te onera? Trouxe basicamente o nosso coletor aí, 1 VM de 6 núcleos, 12 gigas de RAM e 500 gigas de disco. Se a gente olhar o tráfego de Internet, o tráfego de rede, é muito baixo e você pode utilizar ele na sua infraestrutura sem muito onerar o seu orçamento. Basicamente nfdump com nfsen, as outras ferramentas, por exemplo, o LK(F), ele é muito mais pesado. Isso eu posso dizer aí. Tá certo?

Algumas sugestões de leituras que você pode depois conferir, por exemplo, tem exemplos de configurações, tanto para sFlow como IPFIX, para Mikrotik. Você pode consultar o site, ele pode te dar algumas orientações e também a documentação do sourceforge, tanto para nfsen como para nfdump. Obrigado. Não atingi 20 minutos. Agradeço muito toda a paciência, agradeço muito oportunidade. E aí tem os nossos contatos, security@unicamp.br e berto@unicamp.br, se vocês quiserem compartilhar, a gente pode compartilhar também os scripts que a gente utiliza com a comunidade aí. Obrigado a todos.

SR. ANTONIO MARCOS MOREIRAS: Nós é que agradecemos. Gente, agora a nossa próxima apresentação vai ser a do Ricardo Kléber, do Instituto Federal do Rio Grande do Norte. Eu quero reforçar que vocês podem... mesmo os palestrantes não estando agora prestando atenção no chat, vocês podem interagir via chat, porque a nossa equipe está anotando todas as perguntas e questões, a gente está aqui organizando tudo no arquivo para quando acabar essa fase das apresentações iniciais a gente poder colocar essas perguntas para os palestrantes. Gostaria também de reforçar que a gente conta com a ajuda de vocês com o like, né? Temos mais de 800 pessoas assistindo o vídeo, temos menos de 600 likes no vídeo. Isso ajuda as plataformas a distribuírem esse conteúdo para mais gente, fazerem o conteúdo chegar em mais gente. É um conteúdo superimportante, conteúdo de segurança para os provedores, para a gente saber que processos, que ferramentas a gente pode usar dentro dos provedores, dentro das redes, para conseguir tratar toda essa questão que é premente e superimportante. Não adianta só você receber o ataque DDoS lá, receber um outro tipo de segurança e se preocupar com isso na hora, né? Tem uma série de processos e ferramentas que a gente precisa usar, precisa ter no dia a dia para que isso cada vez mais diminua e deixe de acontecer na Internet.

Quero lembrar aqui também, até aproveitando que o Ricardo Kléber é lá do Nordeste, do Rio Grande do Norte, aproveitar para lembrar a vocês, já adiantando aqui alguns avisos, que a gente vai

estar no final do mês com o IX Fórum Regional do Nordeste, em Caruaru, em Pernambuco. E não é tão longe lá da onde o Ricardo Kléber está, né? Então dá para o pessoal do Rio Grande do Norte participar, dá para o pessoal de Pernambuco participar, dá para o pessoal da Paraíba participar, dá para o pessoal de Alagoas participar. E a gente conta com o pessoal dos provedores, o pessoal que participa dos PTTs principalmente, nesse evento. Um evento técnico, com muitas palestras do NIC.br mas tem palestras também do pessoal das CDNs, pessoal da Globo, pessoal do Netflix e outras palestras técnicas de convidados, um evento superinteressante, com bastante networking. E a gente conta com todos vocês lá. Vai ser dia 29 de julho, lá em Caruaru, na universidade federal. Então depois a gente vai colocar o link... aliás, já está o link, NICbrVideos já postou o link no chat, tal, fiquem de olho. Bom, sem mais delongas, vou passar a palavra para o Ricardo Kléber. Ricardo, por favor, assuma. Muito obrigado por ter aceitado o nosso convite.

SR. RICARDO KLÉBER: Olá, pessoal, muito bom dia. Bom dia a todos. Espero que o som esteja ok, a imagem também. Eu estou aqui fora da minha zona de conforto, na iluminação natural, porque eu estou um pouco distante aí do estúdio, mas eu espero que todos estejam me vendo e ouvindo bem aí. Agradecer inicialmente pela oportunidade, mais uma vez de estar no evento do NIC, o convite na pessoa do Eduardo e do Moreiras de estar aqui hoje. Muito obrigado pelo convite. É sempre uma honra, principalmente estar ao lado de feras aí como vocês podem ver, a turma... um evento que começa com a Lucimara já tem aí uma preocupação muito grande de manter o nível, né? Muito bom estar com vocês aí. O Alexandre apresentou o CSIRT da Unicamp, né? Esse nome, CSIRT, CSIRT, CSIRT, né, Lucimara? Isso vem sendo discutindo como que a gente fala esse nome: Grupo de Resposta a Incidentes, enfim. Então é um prazer estar com vocês aqui. E dizer que como é a primeira vez que participo desse evento em si, assim que o Eduardo me chamou, eu fui buscar, contextualizar o que trazer para vocês aqui hoje. Primeiro, como uma Mesa-Redonda, nós não temos aí o tempo elástico para conversar. E a intenção é essa: cada um, então, faça as provocações, dê uma geral aí dentro de sua área de atuação, e a gente, então, depois passa para as perguntas, que é onde a gente espera interagir e tentar ajudar mais esse público. O Eduardo me mostrou, e vendo aí a gravação de eventos anteriores, deu para perceber que o público é muito eclético. E a gente vai falar de incidente de segurança, e diz, onde que a gente foca em um evento como esse? Foquei no meio, para não ter perigo, ficar na zona de conforto, provedores e infraestrutura, mas sem esquecer que temos na audiência estudantes, curiosos, usuários que estão na ponta, que são diretamente e indiretamente muitas vezes afetados com incidentes de segurança e também usuários corporativos, as empresas que têm e precisam se inteirar de problemas de segurança, não deixar tudo na

mão da infraestrutura, afinal de contas, quando o prejuízo vem, vem para todo mundo. Seja para o usuário final, a pessoa física em casa, seja para os provedores que prestam o serviço e precisam dar esse apoio e ficar nesse monitoramento contínuo para identificar, mitigar e responder a incidentes de segurança. E aí também as empresas que cada vez mais são vítimas e precisam estar preparadas para isso. Preparei um material, então, de uma forma mais superficial. Não aprofundei em função do tempo e também desse público. Eu vou fazer uma coisa, nunca vi esse termo, mas seria um coaching dos CSIRTs, dessa fase inicial, provocando, dando palavras-chaves ou colocando o foco aí onde precisa colocar o dedo, para depois a gente abrir a discussão junto com a fala dos demais conferencistas dessa Mesa. E, ao final, quem ficar curioso por um ponto específico que a gente não aprofundou pode, então, solicitar que a gente responde aí, se aprofunda mais, ok? Vou compartilhar aqui, ver se consigo compartilhar aqui dentro desse [ininteligível] aqui que é novo para mim. Acho que agora vai. Sim. Joia.

Então o título já, de antemão, é aquela provocação, eu tenho duas grandes nuances, dois grandes focos para a gente começar a conversar, prevenir e atuar durante o incidente de segurança. E a gente tem que ver, como a própria Lucimara apresentou para vocês aí, que o processo de segurança é um processo que precisa ser visto em todas as suas fases, antes, durante e depois. Se você negligenciar qualquer uma dessas, a gente cai naquela máxima da segurança que é: nenhuma corrente é mais forte que seu elo mais fraco. Você centra fogo na prevenção e depois esquece quando essa barreira é ultrapassada de atuar de forma adequada no combate pós-incidente, o seu elo mais fraco seria aí, e o inverso também, que é o que mais acontece. Quando você não tem uma preocupação preventiva e, de repente, você o que faz, na realidade, é só, quando acontece um incidente, no plano de incidente ver se consegue se recuperar. A gente começa indo aí 25 anos atrás, acho que todo mundo, aqueles mais curiosos, principalmente a nova geração, deve dizer: Espera aí, Lucimara falou aí: o CERT há 25 anos faz esse trabalho. Alexandre falou: O CSIRT, da Unicamp, há 25 anos faz esse trabalho. E esse número cabalístico: 25, o que acontecia antes disso, né, na Internet das cavernas, não havia preocupação com segurança? A gente está nesse contexto exatamente. Boa parte da turma que vocês veem aí, o Moreiras, a Lucimara, o Alexandre e também eu, nessa leva, vem tentando, desde 25 anos atrás, 1997 aí, que vem tentando formalizar, de mãos dadas aí, ninguém solta a mão de ninguém, para tentar formalizar e, juntos, tentarmos melhorar o cenário de insegurança que tem sido uma preocupação cada vez maior.

O Prof. Adriano Cansian, que eu tenho uma admiração fantástica, ele sabe disso, da Unesp, esteve aqui com vocês recentemente no

evento da Intra Rede, tem dito nos últimos encontros do GTS que, hoje, trabalhar com segurança é cada vez mais enxugar gelo. Isso pode ser um pouco fatalista, pode ser um pouco até... parece exagerado, mas o fato é que sempre temos que procurar estar um passo à frente, porque, de fato, pensar somente em segurança como vínhamos pensando antes de 25 anos atrás, quando não tínhamos uma preocupação em ter grupos de resposta a incidentes, e aí está o foco principal de atuação do CERT e acho que é o foco principal também que tem que ser dada atenção em um evento como esse. Se você não tem o seu grupo de resposta, trate de fazê-lo, seja com um, seja com dez, com quantos você puder.

Nesse contexto, 25 anos atrás surgia aí o nosso Naris, eu era... na época estava terminando ali a graduação, recebi a atribuição de tomar conta do firewall da UFRN, da antiga UFRN, minha antiga instituição. E aí montamos o Núcleo de Atendimento e Resposta a Incidentes de Segurança, Naris, e aí ficou já uma piada batida: Se algo não está cheirando bem na sua rede, chame o Naris, e por aí vai.

O fato foi que nesse mesmo período, 25 anos atrás, 97, 98, a gente estava preocupado lá com segurança da informação. E por que achei interessante trazer para cá a história da fundação do Naris? Que vou ser bem breve, para a gente olhar direitinho para não ultrapassar nosso tempo, que eu não estou nem cronometrando aqui propositalmente, para o pessoal da organização ficar louco aí dizendo que eu estourei o tempo. Mas por a gente está falando isso? Porque eu queria que se colocassem no lugar da gente naquele momento. Quem acha: Não, esses caras estão com discurso muito longe. Não tem como. A minha empresa não tem ninguém para trabalhar com segurança. Ah, esses caras estão falando isso porque devem ter grupo com 10, 20, 30 pessoas para trabalhar com resposta a incidentes. Mas não, nossa realidade era e é a da maioria daqueles que começam a pensar em segurança da informação e respostas a incidentes de segurança da informação dentro das suas instituições. Sejam provedores, backbones, sejam empresas, grandes, pequenas, médias, que sejam.

Tudo começou com uma 'euquipe'. E, se você tem essa atribuição ou tem esse interesse em colaborar, em iniciar o seu grupo de resposta a incidente de segurança, procura o CERT para dar esse apoio, que hoje tem apoio muito mais efetivo, e comecem mesmo você sozinho. O Naris começou comigo lá atrás. Era só esse narizinho de nós todos aqui, uma influência do meu pai aqui de Santa Cruz do Inharé, que tem a cabecinha grande e o narizão grande, como podem ver, não é nenhum detalhe de cena. Tanto que a gente bota chapéu para disfarçar o nariz, viu? O pessoal estava perguntando o porquê o chapéu.

Enfim, o Naris começava 25 anos atrás, e rapidamente, veja aí, ele está como um dos únicos do Nordeste, depois veio o CERT Bahia.

Mas nós fomos o primeiro do Nordeste. Depois tivemos: reconhecidos internacionalmente como um dos grupos de resposta a incidente de segurança ativos no país, muito nos orgulhou. E era somente eu. Eu me lembro que nos primeiros eventos de simpósio de segurança na Internet, lá no ITA, a gente fazia a apresentação do que era o grupo de resposta, então tratamento. Aí no final dizia: Quantas pessoas são? Aí eu dizia: Espera aí, nem me lembro, deixa eu contar aqui. Aí sou só eu.

E, gente, não tinha ou não tem, não é necessário, inicialmente, embora seja altamente recomendado, você ser um especialista dedicado a segurança para ter um grupo de resposta. A gente fazia a parte de segurança, mas atendia telefone, colocava cabo de rede, configurava servidor, ainda dava tempo para tomar café e jogar Counter-Strike, né? Na época o CS lá rolava entre os setores da UFRN. Espero que o superintendente não escute isso, que ele não sabia, né, que era na hora do nosso lanche. Enfim, mas comece, se você não tem, aproveita o evento como esse, cola aí no pessoal do CERT e nos demais colegas que estão aqui para ajudar e monta ou fortaleça o seu grupo de resposta a incidentes de segurança.

Eu coloquei aqui: colocando o Naris onde não era chamado, mas que precisava, embora não percebesse. É um outro senso que você tem quando você começa a trabalhar com segurança, você acha que nunca vai acontecer com você, que aquilo nunca vai... que segurança ou incidente de segurança é uma coisa lá distante, para grandes empresas. Cuidado, o usuário final hoje é o foco, as empresas são o foco, os provedores são o foco, todo mundo pode ser vítima disso aí. E aí coloco isso aí, que não é fatalista, né? Qualquer instituição sem o CSIRT começa, inicialmente, por essa percepção de que eu preciso apagar incêndios. Mas e aí, depois que incêndio vem, tem condição de se recuperar ainda? Grandes empresas e também pequenas empresas, algumas com registro, outras nem tanto, tem essa realidade que se acabaram ou tiveram que se reinventar porque foram vítimas, foram alvo de um incidente de segurança, não estavam preparadas e, naquela coisa de "quando acontecer eu vou lá e atuo no incidente de segurança", o incêndio foi grande demais e destruiu todo o capital técnico, muitas vezes a reputação da própria empresa, que algumas aí foram para o espaço, literalmente falando, porque não estavam preparadas.

Pergunta-chave para você usuário, pergunta-chave para você de provedor, para você de empresa: será que eu vou sofrer um incidente de segurança algum dia? O fato é: quando você vai sofrer. E essa é uma provocação que é... eu trago para cá no slide aí em tela cheia, para vocês para que não vejam como fatalista, mas uma realidade. Ainda tem tempo, se você não se preocupa com segurança dentro da sua instituição, independente do tamanho que ela seja. Precisa-se

atuar para que você tenha uma sensação, pelo menos a sensação, como dizia o Prof. Adriano, né, de que está enxugando gelo, de que está minimamente preparado e que vai conseguir sobreviver minimizando as consequências desse cenário que está cada vez mais nebuloso. Nós temos tecnologias emergentes aí que trazem junto com ela diversas novas preocupações, então estar preparado é uma questão diária, um pensamento diário. E aí, claro, a gente bota esses prints aí que todos têm conhecimentos, que estão aí todos os dias nos grandes blogs e veículos de comunicação, a quantidade de empresas ou de instituições dos mais diversos portes que têm prejuízos aí faraônicos quando se fala de ataques e incidentes de segurança.

Se vocês procurarem aí, depois no final tem aí o link de alguns dos meus canais no YouTube, algumas palestras que dei no Campus Party, [ininteligível], no GTS, vocês vão ver, eu falei sobre ransomware alguns anos atrás, está cada vez mais frequente e recente. E digo que é um dos pontos principais que se deve concentrar a atenção, que é a prevenção e, também, quando você é vítima de ransomware, seja pessoa física, pessoa jurídica ou provedor, o que você precisa fazer, tem que estar atento para isso aí. Mas nós temos diversas outras situações ou diversos outros perigos atuais aí. Temos as portas abertas para uma nova realidade com IoT, com IPv6, com... a segurança por perímetro foi para o espaço, você não sabe mais de onde aquilo está vindo, porque o ataque pode estar vindo de uma geladeira IoT, pode estar vindo de um smartwatch, pode estar vindo até de um controle de portão, se for o caso, ligado em rede, mas em qualquer situação que seja... Isso só nos leva a ter cada vez mais essa consciência, ou precisar ter essa consciência de que segurança é um processo de preocupação contínuo.

Palavras de ordem, três. Acho que vocês escutaram a Lucimara falar, escutaram o Alexandre falar da questão da proatividade. Acabou, não tem mais essa coisa de você, precisa-se estar sempre um passo à frente. E, para estar um passo à frente, vem a segunda palavra de ordem, a questão da capacitação. É necessário constantemente se capacitar, estar atualizado com tecnologias com segurança ou tecnologias de segurança, procedimentos para que você possa estar com esse passo à frente. E cooperação. Ninguém resolve problema de segurança sozinho. Principalmente com seu provedor; se você é provedor, com seu backbone, com outros parceiros provedores, não vejam parceiros provedores concorrentes como inimigos, mas parceiros da hora de tratar incidentes. Vocês podem estar tendo o mesmo problema e podem tratar juntos isso aí.

E há algum tempo atrás a gente falava que segurança da informação tinha duas vertentes bem antagônicas, que era a questão da segurança ativa e a preventiva. Grupo de resposta a incidentes era uma coisa que você esperava acontecer para estar preparado. E, do

outro lado, vinham a questão dos *ethical hackers* com pentests. E hoje a gente vê que isso converge, a equipe de segurança tem que estar, sim, não só antenada na sua prevenção e na sua capacidade de responder a incidente de segurança, mas também ela tem que estar preocupada dentro da sua empresa, fazendo pentests internos, análises de incidentes internos. Veja que as empresas cada vez mais disponibilizam programas de *bug bounty*, né? Chamam hackers, *ethical hackers* para encontrar furos e brechas nas suas instituições e bonificam essas pessoas por isso, porque é necessário estar em todas as frentes. Não mais só naquela retaguarda. Incidente de segurança passou a ser visto também, ou tratamento de incidente, também, como um processo que você precisa ir para o ataque, como Sun Tzu falava na Arte da Guerra: "Você tem que conhecer o inimigo, mas também... Se conhece o inimigo e a si mesmo, não tema o resultado de cem batalhas. Se conhece a você, mas não ao inimigo, para cada vitória, sofrerá uma derrota. Se não conhece nem ao inimigo, nem a si, perderá todas as lutas". Traz isso para dentro do teu contexto, você vai ver que não tem nada de exagero, é essa a nossa realidade.

Algumas questões de motivação, coloquei aí questões pontuais para a gente seguir aqui. Eu vou só parar de compartilhar aqui para dar uma olhada no chat, porque eu estou totalmente desconectado do meu tempo aqui. Deixa eu dar uma olhadinha só... retornar aqui para ver o meu tempo. Ok, tranquilo. Eu vou voltar aqui a compartilhar. Desculpem aí, pessoal. A gente acostuma a trabalhar com dois monitores, aí... ok.

Então, vamos lá. Algumas questões de motivação: o aumento generalizado na quantidade de diversidade de incidentes de segurança. Isso é um fato. A quantidade de variedade de organizações sendo afetadas por incidentes de segurança em sistemas computacionais, não são só os grandes mas também pequenos, aqueles que estão começando, que estão muito tempo no mercado. Mas felizmente há uma maior consciência por parte das organizações, da necessidade de políticas e práticas de segurança, mas às vezes não se sabe como é que se coloca em prática isso. Procura o apoio especializado aí do CERT para montar o seu grupo e trabalha com cooperação. A palavra-chave, ou as palavras-chaves são essas.

Nós temos aí legislações recentes, desde o marco civil em que o Comitê Gestor trabalhou ativamente aí, mas mais recentemente a LGPD com essa necessidade, esse novo mercado que se abre para proteção de dados pessoais e que tem que ser pensada de forma profissional dentro da empresa, sob pena, inclusive, de incidir em situações que a empresa tenha de arcar com o ressarcimento financeiro por não estar cumprindo a legislação da LGPD. E essa percepção de que os administradores de redes e sistemas não podem

se proteger sozinhos, os sistemas e as informações da organização. Cooperação, a palavra-chave.

Caminhar aqui para o final, estou com dois minutinhos aqui. O que é o CSIRT, como a Lucimara deu uma geral e o Alexandre mostrou que é implementado lá na Unicamp, um ponto único de contato na rede para comunicar problemas de segurança. É necessário que o seu usuário, sejam os usuários finais, mas também suas equipes, seus departamentos dentro da sua instituição saibam a quem recorrer na hora que tiver um problema de segurança. Que se tenha uma condição de classificar na hora da atuação, você tem incidentes de maior e de menor gravidade, e classificar isso para saber onde agir primeiro é fundamental, e só um trabalho planejamento, a gente consegue fazer isso. Existem, felizmente, várias normas padrões, a Lucimara colocou bem aí, e eu coloco no final da apresentação duas RFCs que foram preparadas para auxiliar nesse processo de utilização de normas, tratamento e notificações internas e externas, ou seja, preocupa-se com o teu público-alvo ou teu público final, o provedor deve se preocupar com o usuário e também com sua infraestrutura, e também, naturalmente, com aqueles agentes externos que são alvo do seu ambiente interno ou que atacam seus usuários ou seus ambientes, notificação de incidentes para a gente ter estatísticas mais aprimoradas e o monitoramento contínuo.

Respostas... finalizando aí, ações contínuas. Respostas a incidentes, atendimento a demandas internas e externas. Não podemos deixar de ter, acho que isso é fundamental, além do firewall, IDS, sejam IDSs de rede, mas também IDSs de host, IDSs wireless, dentro da sua infraestrutura, integrados com servidores de log, os logs hosts. Como a gente falava, pentests e análises de vulnerabilidades internas, se você não tem uma equipe para isso, fala com a gestão para contratar um pentest externo para ver como está a tua segurança para evitar ou mitigar, minimizar a possibilidade de incidente de segurança. Ficar atento aos boletins, emissão de alertas e advertências e repassar isso para teu público interno. Desenvolver e adaptar ferramentas de segurança, dependendo da maturidade do teu centro de resposta de incidentes e disseminar informações relacionadas à segurança. O CSIRT faz muito bem com suas cartilhas, com seus eventos, como o Moreiras colocou agora há pouco.

Os slides vão estar aí para vocês. Aqui tem um resumozinho do passo a passo do processo de gestão de incidentes de segurança da informação. Aqueles que tiverem curiosidade e dúvidas sobre cada passo desse aqui, pode acionar a gente aí nas perguntas, em seguida, ou depois. Os nossos contatos estão aí no final. Aí as duas RFCs que a gente falava agora há pouco, uma específica para grupo de resposta a incidentes, a RFC 2350 e a 2196, que é um livro de cabeceira aí para segurança de sites, também na forma de RFC.

O CERT é nosso porto seguro, quando fala, no Brasil, quem quer criar e manter um grupo de resposta a incidentes e tem uma base consolidada aí, uma concentração de esforços. Mantém-se junto em cooperação com o CERT que você já está em um bom caminho. A página do CERT/CSIRT tem muito material legal, tá? Quem está começando e começar a [ininteligível] cada tópico desse, de estatísticas, o curso, os projetos, vocês vão ver aí que tem material para se passar vários meses se atualizando ou se inteirando do que é o CSIRT. E aí estão os meus contatos para quem quiser conversar pós-palestra. Meu site e meu e-mail principal que está aí. Instagram, né? O Pessoal mais antigo... Eu entrei no Instagram, não gostava de usar, achava muito evasivo, mas vou ter que dar meu Instagram também. E os meus três canais no YouTube, para quem quiser ver palestras anteriores, aulas do IFRN que eu disponibilizo e questões pessoais que não estão associadas diretamente a isso aí.

Bom, pessoal, vou deixar, então, o espaço para o complemento da Mesa. E eu estou à disposição, depois, para as perguntas, quando a gente encerrar essa primeira etapa. Obrigado, desculpa ter estourado o tempo, pessoal.

SR. EDUARDO BARASAL MORALES: Obrigado, Ricardo. Bom, antes de a gente chamar próximo palestrante, eu gostaria só de dar os avisos, que eu vi que tem muita gente perguntando no chat. Então, quem quiser o certificado precisa se inscrever no link que está sendo colocado no chat, tá? E ficar atento até as 14h no seu e-mail. Por quê? Porque tem um link ali de retorno. Você tem que clicar naquele link. Temos também os sorteios, tá? Nesse mesmo link do certificado, você está concorrendo também ao sorteio do kit NIC com os patrocinadores. E, inclusive, dos kits extras. O kit NIC era um conjunto com camisa, lapiseira, adesivo, caneca, kit de ferramentas, carregador e livrinhos. Os kits extras são ali a senha de acesso do Super Conhecimento e o desconto de 25% no curso de Segurança de Redes da VLSM Solintel. Temos também o sorteio, pessoal, da Globo, tá? Que é um voucher de acesso grátis por dois meses ao Globoplay, válido somente para novos assinantes. E temos também o da 4Linux, que é um curso da 4Linux à escolha do ganhador. Então, são vários sorteios. Quem quiser, vai se inscrevendo. Bom, para a gente não atrasar muito aqui, gostaria de chamar nosso próximo palestrante, que é o Lacier Dias. Lacier, fica à vontade.

SR. LACIER DIAS: Obrigado, meus queridos. Sempre uma honra estar aqui com vocês, aceitar esse convite. E, sem mais delongas, como bem colocou nossa querida Lucimara, vamos ao desafio de compartilhar a tela. Desafio concluído aqui, pelo que me parece, deu certo. Bom, vamos lá. Então muita coisa já foi dita pelos nossos amigos. E, de fato, falar, assim, mais para o finalzinho, eu acho um pouquinho mais detalhado. Então, eu resolvi abordar coisas mais

até vou chamar de práticas, tá? Eu trabalho com provedores de Internet há muitos anos. E a gente vê os provedores de Internet sofrendo muito com relação a ataques, né? Embora o CERT tenha treinamento, o Registro tenha treinamento, o NIC tem treinamento, toda a operação NIC.br tem vários treinamentos, ainda assim existem muitas dificuldades a serem transpostas e muitas ferramentas que não chegam até os provedores por diversos motivos. Então, eu concatenei algumas que eu entendo que são essenciais e mínimas para que o provedor tenha ali uma noção do que ele pode fazer e do que efetivamente ele consegue operacionalizar dentro do seu provedor de forma mais simples, né, do que uma ferramenta, talvez, com um grau de complexidade maior.

Minha apresentação aqui resolveu... Agora resolveu funcionar. Eu amo o ao vivo por causa disso. Então, vamos lá. Brasil, nosso querido país aí, é o país com maior volume de ataque cibernético que a gente tem visto ultimamente, né? E 35 milhões de ataques cibernéticos são realizados por meio de acesso remoto durante a pandemia. Então eu estou fazendo alguns indicadores, porque são dados que muitas vezes, como o professor falou antes de mim, não é que você não foi atacado, é quando você vai ser atacado. Porque muito provedor tem um comportamento de "não, só acontece com o vizinho. Comigo nunca acontece".

Então, assim, é muito importante entender que várias pontas estão fazendo o seu trabalho. Então a polícia está fazendo o trabalho dela, o Registro.br, o CERT.br está fazendo trabalho dele, várias funções fazendo o seu trabalho e o provedor também tem que fazer o trabalho dele para poder ajudar, por quê? Porque o provedor de Internet, ele tem vários portes. A gente tem provedores enormes, que se assemelham a operadoras, e existem provedores que o camarada tem 500 acessos. E aí ele tem um roteador para autenticar, um roteador para fazer o compartilhamento da Internet, porque não tem mais IPv4. Então vários provedores estão em cima de NAT, né? E acabou, essa é a estrutura do provedor do cara. E ele tem 500 famílias que confiam nele, 300 famílias que confiam nele, mil famílias que confiam nele. E essas famílias têm informação, têm capacidade computacional, tem 'Skygato' minerando Bitcoin dentro de casa. Então assim, precisa ter um olhar para esse universo também da operação pequenininha.

Então ataques hackers, como teve Presidente Kennedy. "A polícia prende empresário suspeito de ataques cibernético a operadoras em Goiânia". "Hackers exploram vulnerabilidades antigas, diz Trend Micro", então isso é uma outra coisa que é problema, a atualização, ela precisa ser feita. O provedor tem uma dificuldade extrema em fazer atualização do seu parque de equipamentos. Ele prefere comprar um equipamento novo do que atualizar. E isso a gente está falando de

backbone, você imagina quando a gente fala de ONU, que é uma por família. O equipamento está lá dentro da casa do cliente, o provedor nem lembra mais que aquele equipamento está lá e aquilo fica em uma versão da idade da pedra, com várias vulnerabilidades.

Então, para fazer isso, a gente tem aqui, eu trouxe algumas dicas. A maioria esmagadora delas gratuitas que eu definitivamente não sei o porquê o provedor não participa. Então, provedor, querido, você que está me ouvindo, principalmente os donos de provedor, se você não sabe nenhuma informação dessa que eu vou passar aqui, se você nunca viu um site desse, se a sua equipe nunca te falou disso aqui, você tem um problema grave aí dentro, tá? Gravíssimo, inclusive. Porque o MANRS, por exemplo, é de graça. Você cumpre algumas regras e passa a fazer parte da comunidade. É gratuito, vai lá, entra no site, cumpra as regras que você consegue fazer parte dessa comunidade e mitigar vários lixos que podem aí estar dentro da sua estrutura.

A gente tem o TRS, é um serviço antigo da Team Cymru, que também é de graça. Você recebe, através de uma sessão BGP, aí o cara já tem que ser autonomous-system, tem que ser AS, então você recebe ali uma tabela de lixo que ajuda a mitigar vários níveis de ataques e lixos que sua a rede possa tanto enviar quanto receber. Que a gente não tem como ser babá dos nossos clientes. Então, não tem jeito, a gente precisa ter mecanismo no meio do caminho para que isso possa ser mitigado.

A gente tem o Walled Garden, também é uma ferramenta que trata lixo, filtra lixo, tem suporte em português, que você pode entrar em contato, testar ali o nível de segurança que está o seu AS e também fazer parte da comunidade, trocando informações sobre lixo dentro da sua estrutura e recebendo tabelas de lixo também para poder exatamente minimizar essa questão do tráfego de lixo que você está fomentando aí, tráfego prejudicial à infraestrutura da Internet.

A gente tem o BCP.NIC.br, que a própria chamada do site eu já acho maravilhosa. Que é um portal que reúne o conjunto de boas práticas operacionais ainda não são adotados amplamente pelos ASs brasileiros. Por quê? Essa é a pergunta-chave. Eu sei que o cara está preocupado em vender, eu sei que está preocupado em instalar. Eu sei que está preocupado em reter cliente. Mas isso aqui faz parte da retenção do cliente, porque se sua rede for instável, sua tiver problema, sua rede fica caindo, sua rede tiver baixa experiência de uso e o seu cliente vai trocar de provedor. Então isso aqui faz parte do seu processo de retenção de clientes. Isso não é um luxo, entendeu?

É porque, infelizmente, a gente não tem aí uma mão mais pesada com relação à segurança em cima de provedores. Porque falta um pouco de conscientização, embora gaste-se muito tempo ou muitas

pessoas relevantes no mercado dedicam suas vidas para divulgar essa informação, e haja vista a idade do projeto Naris ali, que achei maravilhoso o nome. Então assim, não é de hoje que pessoal está falando em segurança. Não é de hoje que o pessoal está trabalhando em cima disso. A gente tem o Qrator, que essa é uma das ferramentas que acho mais legal, porque qualquer modificação que acontece no seu bloco, ele vai te avisar. Qualquer tráfego estranho que possa manipular sua tabela... perdão, seus anúncios, ele vai avisar. Também é um serviço que é gratuito.

Então, assim, são ferramentas que vão facilitar sua vida e na hora que você tiver uma infelicidade de passar por um ataque, ou passar por um desconforto na sua infraestrutura, essas ferramentas vão municiar de informação para que você possa reagir rápido, para que você possa, de repente, antever. Porque o cara não acorda segunda-feira de manhã e fala: Vou atacar o provedor X, Y e Z. Existe uma análise, ele faz um scanner, ele fica analisando o cenário, ele olha os anúncios do bloco, ele coleta um monte de informação que fica aberta na Internet. Ele faz todo trabalho de análise antes, para quê? Para o ataque ter sucesso. Então esse atacante que a gente tem na imaginação, que tem um poder supremo, que é quase o Neo da Matrix, que ele vai lá e 'shazan', derruba o provedor, isso não existe, entendeu? Infelizmente é um cara intelectualmente privilegiado que usa esse intelecto para o mal. Isso é um atacante mais recente. Não é aquele gordo, nerd, sentado na frente do computador que não tem o que fazer. Não, infelizmente, agora os caras têm um nível, infelizmente, profissional cada vez maior. Por quê? Porque virou uma fonte de receita. E a gente precisa cessar essa fonte. Porque enquanto tiver dinheiro... Eles não fazem por esporte, eles fazem porque tem receita. Eles fazem porque circula dinheiro. Eles fazem porque inúmeros provedores vão lá e pagam resgate, pagam para parar de ser atacado. É por isso que é feito. Porque se ninguém pagasse, se não movimentasse dinheiro, não tinha motivo.

E a segurança da Internet é um desafio de todos, todos. E ações coletivas tendem a ser mais eficientes em mitigar e resolver os problemas relacionados à segurança. Então não adianta a gente tentar achar que vai responder todo mundo sozinho, resolver tudo sozinho, porque não vai. Vai ser muito mais fácil a gente conseguir parar de achar que o coleguinha provedor é nosso inimigo e fazer uma ação aí mais coletiva para que a gente possa ter um sucesso maior em resolver esse problema. Então, muito obrigado a todos. Muito obrigado pelo convite. E passo a bola aí de volta para a equipe aí, com o Eduardo.

SR. EDUARDO BARASAL MORALES: Obrigado, Lacier. Moreiras, pode continuar, fica à vontade.

SR. ANTONIO MARCOS MOREIRAS: Obrigado, Eduardo. Obrigado, Lacier. E agora nós vamos para o nosso último palestrante. Antes de a gente fazer a interação e de a gente ir para as perguntas. E o nosso palestrante é o Marcello Zillo Neto, que é da AWS, da Amazon Web Services. Marcello, pode seguir aí.

SR. MARCELLO ZILLO NETO: Legal. Primeiro agradecer o convite e falar que é um desafio, enquanto eu vou compartilhando a tela aqui, né? Que é um desafio falar depois dessas feras todas, né? Depois da Lucimara, do Alexandre, do Ricardo, do próprio Lacier. Então, prazer estar aqui com vocês. E nosso papo aqui pelos próximos 10, 15 minutos, o objetivo é de a gente falar um pouquinho sobre segurança no ambiente de nuvem. E aí eu fui tomando nota de várias coisas que os colegas foram falando e eu vou tentar, na medida do possível, tocar isso no que isso significa no ambiente de nuvem.

A Lucimara, por exemplo, falou com muita propriedade sobre a questão de segundo fator de autenticação, né? O MFA, a importância de você utilizar o segundo fator de autenticação. E eu costumo dizer que ao adotar serviços de nuvem pública, a identidade passa a ser ainda mais importante. Porque a identidade digital é o que autentica suas aplicações, os seus usuários, os seus endpoints, os seus sistemas para usar os recursos que estão disponíveis na nuvem. E aí vem uma questão que o Lacier colocou e alguns outros palestrantes colocaram, que diz respeito a muitas vezes usar controles que já estão disponíveis. E a gente vai ver que existem muitos controles de segurança que é o que a gente chama de cloud-native security controls, ou seja, existem controles de segurança nativos na nuvem que podem ser utilizados para aumentar o seu nível de resiliência.

E aí sempre gosto de começar a conversa falando um pouquinho sobre uma missão que eu acho que todos nós cada vez temos mais que é: talvez no passado a gente falava muito em: Tem que ser ágil ou tem que estar seguro? Hoje em dia isso não é realidade, hoje as duas coisas têm que acontecer. As empresas querem ser ágeis, as empresas precisam ser ágeis e elas precisam estar seguras ao mesmo tempo. E aí a primeira coisa que eu falo para vocês é: ambientes de nuvem pública, como no caso da AWS, foram criados com vários princípios de segurança nativos. Que, novamente, precisam ser considerados quando você vai adotar serviços de nuvem pública. Quando você fala de serviço de nuvem AWS, por exemplo, todas as solicitações que você faz, criar um servidor, criar um usuário, deletar um usuário, provisionar um determinado recurso de storage, tudo isso é 'logado' nativamente.

Existe um recurso que chama cloud trail, já que no ambiente de nuvem, no ambiente de nuvem pública tudo o que acontece é uma chamada de API. Cada vez mais a gente vê API sendo o mecanismo de

automação, de escala, de provisionamento, e aí a gente começa a falar muito em segurança de nuvem, e a lembrar também que passa a se discutir muito segurança como código. Se eu provisiono um recurso no ambiente de nuvem, por que não os provisionar já com os princípios e com os recursos de segurança nativos? E todos nós aqui da área de segurança, tem gente com muito tempo de experiência aqui, né, poxa, isso é muito legal, acho que vamos concordar que sempre a gente vem falando sobre a questão do security by design. Como eu vou implementar segurança desde o dia zero com os princípios de segurança mínimos, ou princípios de segurança básicos?

Então, a nuvem proporciona fazer isso. No entanto, eu sempre gosto de trazer aqui, no primeiro momento, a discussão do que a gente chama do modelo de responsabilidade compartilhada. Porque aqui a gente precisa tomar um cuidado, quando a gente está falando de segurança em ambiente de nuvem. Você pode ter os dois extremos. Eu já peguei casos de clientes, enfim, ou alunos, que imaginam que a segurança é toda responsabilidade do provedor, e já peguei o oposto também, dizendo: poxa, então a segurança é toda responsabilidade minha. Esse é um padrão de mercado que foi criado pela AWS, quando a AWS foi concebida, muitos anos atrás. E a gente definiu um padrão que é o que a gente chama de segurança na nuvem e segurança da nuvem. O que significa isso? O usuário, o cliente, ele tem responsabilidade de segurança dependendo dos... e elas são diferentes, dependendo dos serviços que ele utiliza. E eu vou trazer alguns exemplos para a gente aqui. Que é o que a gente chama de segurança na nuvem. Ou seja, vou dar um exemplo: proteger os dados, criptografar os dados, controlar acesso aos seus dados no ambiente de nuvem. Quem é a melhor pessoa para controlar o acesso? O dono do dado. Aquele que é responsável pelo dado. E aí existem mecanismos que o provedor de nuvem, no caso a AWS, proporciona para você fazer esse tipo de controle.

Então, segurança na nuvem é aquilo que o cliente tem que fazer. E a gente tem aí segurança da nuvem. Que é o que provedor faz nativamente. Eu vou explicar com mais detalhes, mas depois no material que vão receber tem os links que detalham todos esses modelos de responsabilidade compartilhada. E eles vão basicamente camada a camada. Mas o que é importante a gente saber? Quando a gente está falando de segurança em nuvem, o provedor, ele tem responsabilidades, sim. Em qualquer cenário, ele vai ter, por exemplo, responsabilidade quanto à segurança do Data Center. Quem é responsável por garantir ou controlar quem acessa o ambiente? Se um HD sai de uma determinada máquina com defeito, como você destrói? O provedor, no caso a AWS, ele tem padrões internacionais para destruição de dados em casos de necessidade de manutenção. O provedor, no caso a AWS, tem que prover o que a gente chama de

multi-tenant, ou seja, se eu tenho duas ou três instituições na mesma zona de disponibilidade, no mesmo Data Center e na mesma região, elas estão isoladas. Mesmo que elas estejam fisicamente no mesmo lugar, duas instituições distintas, o impacto de uma não deve causar impacto na outra. E aí tem tantas outras responsabilidades que a gente poderia dizer como, por exemplo, atualização de patch de roteador, atualização de patch de firmware e de hardware, de storage. Ou seja, tem várias coisas que o provedor nativamente vai fazer.

E uma das coisas que a gente tem que lembrar sempre, e eu gosto de enfatizar isso, é que em qualquer situação, vocês vão ver, em qualquer situação o cliente, ou seja o dono do dado, ele vai ter uma responsabilidade que é de dizer quem pode ter acesso ou não ao dado e onde ele está, ou seja, criptografar, isolar. E responsabilidade sobre o endpoint. Ou seja, no final, você sempre tem alguém, uma entidade, um computador, um OIT, um dispositivo, uma aplicação que acessa o ambiente de nuvem. Então você tem que controlar a segurança desse endpoint. E, não menos importante, a gestão de identidade do ambiente, você vai ter que controlar isso. Então, minimamente, o que a gente costumava dizer há muitos anos já na área de segurança, o quão importante era fazer gestão de acesso, na nuvem é ainda mais importante. Porque toda vez que você tem uma chamada em uma API para executar uma atividade, você precisa se autenticar. E a pergunta é: como você se está autenticando, só com usuário e senha? Lembrando que, caso da AWS, por exemplo, o multi-factor authenticator não tem custo adicional, é um recurso que está disponível para ser utilizado. E muitas vezes os usuários, as empresas não utilizam.

Agora vamos pegar um exemplo prático que acho que faz sentido a gente fazer esse comparativo. Se a gente olhar no dia a dia, pensar em uma base de dados tradicional. Quando você olha para o ambiente tradicional, você tem todas essas responsabilidades, desde a segurança física até a segurança da aplicação que está acessando aquela base de dados. Quando você começa a migrar os serviços para a nuvem pública, você faz uma das coisas que a gente chama de *heavy lifting*, ou seja, você pode: algumas responsabilidades, dependendo do serviço que você usa, passam para o seu provedor, nesse caso a AWS. Então quando você está usando IaS, infraestrutura como serviço, naturalmente segurança do hardware, segurança física, até onde a escala sistema operacional, isso é responsabilidade do provedor da AWS. Então, se eu pegar banco de dados na rede tradicional e levar para a rede pública, o modo de infraestrutura como serviço, eu transfiro algumas responsabilidades para o provedor, mas tudo que está em azul aí continua sendo responsabilidade minha. Veja lá, controle de acesso, escalabilidade, alta disponibilidade, backup, gestão de banco de dados, a instalação de bancos, gestão de SO, patch, que

a Lucimara falou tanto, e realmente, a gente vê que MFA e patch são dois pilares importantes que devem ser considerados.

E existem também casos onde você não quer ter tanta responsabilidade de segurança e você quer usar o que a gente chama de serviços com maior valor agregado. Então, vamos pegar aqui o que chama de plataform as a service. Você vai usar um serviço de banco de dados gerenciado pelo seu provedor. No nosso caso aqui, um exemplo, o RDS. Vejam a quantidade de coisas que passa a ser responsabilidade do provedor. Mas vejam que ainda assim controle de acesso e elasticidade continuam sendo responsabilidade do cliente. Por quê? Porque somente o cliente consegue dizer quem pode acessar o quê, quando e onde. E é fato que à medida que você vai subindo, ou seja, você começa a utilizar serviços com ainda mais valor agregado, o que a gente chama de serviços abstratos, você, por exemplo, talvez não tenha que se preocupar mais com elasticidade.

Então, no final das contas, as empresas que vão para a nuvem pública, tem vários fatores, o que a gente chama de *business drives* para a adoção. Às vezes, redução de custos, às vezes... muitas vezes, na verdade, redução de custo, a otimização, ganhar agilidade, implementar modelos de *deploy* de funcionalidades de forma mais ágil. E segurança pode ser um fator também. Porque na medida em que migra... Vamos pegar esse exemplo aqui, deixa eu voltar no slide anterior. Vamos pegar esse exemplo de banco de dados aqui, que eu usar o banco de dados como serviço. A Lucimara colocou bem a questão dos patches. Será que eu quero continuar aplicando patch ou será que eu vou transferir essa responsabilidade para o provedor de serviço? Se eu estiver usando o serviço de infraestrutura como serviço, isso não é possível. Mas se eu estiver usando alguns modelos com maior valor agregado, óbvio que vai ser muito mais factível eu ter esse tipo de transferência. E aí se a gente pudesse resumir, basicamente na medida em que vai subindo, né, você tem menos responsabilidades, mas continua ainda com a responsabilidade de criptografia dos dados, proteção do dado, acesso, ou seja, gestão de acesso continua sendo uma responsabilidade importante. Lembrando que na nuvem pública a gente tem conceito do control plane e do data plane. Ou seja, o control plane, que é a interface de gestão, ela está conectada à Internet por funcionalidade, porque ela precisa ser acessada de qualquer lugar, o que não significa que qualquer um acessa. Você pode controlar por regras de IP, você pode controlar por [ininteligível], você pode controlar por diferentes mecanismos de solicitação de execução de alguma atividade. Então, na prática, é importante entender detalhadamente esse modelo de responsabilidade compartilhada na medida em que você começa a adotar serviços de nuvens públicas, no caso da AWS.

E aí vale destacar o seguinte, quando a gente fala de proteção de dados, nós que trabalhamos com segurança, se perguntar para todos nós, a gente gostaria que o dado estivesse encriptado sempre, *end-to-end encryption*, dado sempre protegido. Só que muitas vezes a gente esbarra com limitações que são limitações muitas vezes tecnológicas que não permitem criptografar por uma questão de performance, por uma questão de interoperabilidade, enfim. A nuvem pública, nuvem AWS, permite fazer o que a gente chama de criptografia em escala. Então, você pode criptografar o dado *end-to-end*. Ele pode estar criptografado na base, ele pode estar criptografado no storage, ele pode estar criptografado no volume, ele pode estar criptografado no trânsito, e isso faz com que você tenha, inclusive, um maior nível de segurança de segurança dos dados que estão armazenados. Existe, inclusive, um mecanismo que a gente chama de *bring your own key*. Você pode criptografar com sua própria chave criptográfica dentro do modelo de Cloud HSM.

Agora, até para otimizar nosso tempo aqui, que depois vocês vão receber todo o material completo. Eu sempre gosto de trazer para a discussão o que eu chamo de pilares de cloud security. Comentário importante, quando a gente fala de implementar segurança no ambiente de nuvem pública, não é a mesma coisa que implementar segurança no ambiente tradicional. Eu gosto de usar um exemplo onde você tem... você mora em um condomínio de casas, aí você muda para um condomínio de apartamentos. No condomínio de casas, você dorme, come, sai, faz um monte de coisas. E no condomínio de apartamento também. Eu passei por isso recentemente, mudando de casa para apartamento. Só que o como você faz muda.

Então vou pegar o exemplo aqui da resposta a incidente. Você vai ter que fazer resposta a eventos de segurança, a possíveis eventos que podem acontecer no seu ambiente. Mas você vai fazer do mesmo jeito? Onde estão os logs? Estão nos mesmos lugares que você está acostumado? Até o Alexandre colocou bem, né, a questão do treinamento, né? As pessoas estão treinadas para responder um evento de segurança no caso de ambientes de nuvem pública? Então, tem três pilares que são fundamentais, o primeiro deles é o que eu chamo de visibilidade. E acho que o Alexandre e o Ricardo trouxeram esse ponto, da importância de você ter visibilidade do que acontece no seu ambiente, do que é normal e do que não é.

No caso da AWS, você tem mecanismos para fazer esse inventário não só de ativos mas também para entender comportamentos anômalos de autenticação de usuários, de aplicações, de workloads. O segundo é que a nuvem te proporciona automação, automação em larga escala. E isso está muito relacionado, muito relacionado à resposta a incidente. Até porque no ambiente de nuvem pública, muitas vezes, o que você quer é ter escalabilidade, né? Você

começa o dia com três contêineres, no meio do dia você tem duzentos, no final do dia você 5 mil, e durante a madrugada você tem três contêineres. A pergunta é: como você automatiza a resposta a um evento de segurança especialmente em ambientes que muitas vezes são efêmeros? Onde você pode ter é escala. A máquina sobe e desce, e como você garante que aquele contêiner, que aquela máquina sube com todos os controles de segurança nativos? A automação te permite fazer isso. Por isso é que a gente fala muito quando a gente comenta sobre segurança em nuvem, de segurança como código. Você passa a pegar as políticas de segurança que estão escritas em papel e transformá-las em códigos que vão automaticamente implementar os seus controles de segurança. E, sem dúvida, você busca maior resiliência. E existem diversos mecanismos para aumentar o seu nível de resiliência. A gente falou aqui no caso de... acho até que foi o Alexandre que comentou sobre a questão de ataque de negação de serviço. A AWS proporciona, por exemplo, uma camada de proteção DDoS sem custo, que protege contra ataques de alto volume, enfim. Dependendo do nível de ataque, talvez você tenha que ter algumas outras camadas adicionais, que aí tem outros serviços que podem ajudar a fazer isso, mas existe, sim, nativamente, diversos serviços que ajudam você a implementar um ambiente com maior visibilidade, automatizar a implementação de segurança, usando modelos de API, segurança como software e também aumentar a resiliência.

Não é o nosso objetivo, eu não vou passar por esse slide, vou passar voando por ele, porque eu já estou terminando. Mas a minha recomendação para todos os clientes ou para todo mundo que vai começar a usar serviços de nuvem pública, serviços de nuvem AWS é: é importante que vocês conheçam os mecanismos de segurança nativos. Quando a gente fala de nuvem AWS, existem recursos de gestão de acesso, que alguns deles não têm custo adicional, controles de detecção, então a gente falou assim: Poxa, eu preciso detectar o que é comportamento anômalo, pois é, existe um serviço que se chama GuardDuty que ele analisa o comportamento dos seus workloads e gera alertas em tempo real de possíveis anomalias. Assim como você tem serviços de segurança de infraestrutura, serviço de segurança de proteção de dados, serviço de segurança para resposta a incidente. Ou seja, existe um conjunto muito grande de recursos que podem ser utilizados para te ajudar no processo de resposta; detecção, resposta, mitigação e ter mais agilidade. Eu mencionei o GuardDuty, é um exemplo, porque ele realmente pega sinais dessas APIs, de tráfegos, de comportamentos anômalos e aí a gente tem um aliado muito grande para segurança, que são os modelos de machine learning, de inteligência artificial, que vão basicamente usar todos esses dados para a tomada de decisão.

E, para eu fechar, esse é só um exemplo do que a nuvem traz como automação. Você pode analisar não conformidades de políticas de segurança do seu ambiente, de fora, automatizada em tempo real. Se alguém subir um recurso, um servidor, um contêiner, um usuário sem os padrões mínimos de segurança, automaticamente você pode gerar um alerta. O que eu costumo dizer é assim: Às vezes você descobre uma falha de configuração de segurança ou quando você faz um pentest ou quando tem um incidente, ou quando tem uma auditoria, ou seja, qualquer um desses cenários não é bom. Então a nuvem te permite criar políticas que vão ser avaliadas cada vez que um recurso é disponibilizado no ambiente.

E se vocês esqueceram tudo o que eu disse, agora é hora de acordar, como dizia um velho amigo meu, você pode estar mais... tão ou mais seguro na nuvem quanto a gente fala em ambientes tradicionais. E aí você pode ter, inclusive, a otimização quando a gente fala de custos operacionais. O que é preciso ter em mente? Conheça o modelo de responsabilidade compartilhada. Vocês vão receber um material com um link com mais detalhes. É importante entender quais são os serviços nativos que estão disponíveis. É importante entender como esses serviços estão integrados, entender se as soluções da própria AWS ou de parceiros precisam ser utilizadas para aumentar o seu nível de resiliência. E lembrar que a nuvem te dá visibilidade, te permite controle em larga escala de criptografia do dado, gestão da identidade, automação e mecanismos de resiliência.

E aí a gente falou bastante de resposta a incidente, eu gosto sempre de usar esse exemplo, porque a resposta a incidente, eu tenho caso real de um cliente aqui no Brasil que, ao detectar um malware em um servidor, automaticamente ele [ininteligível] uma outra instância, isola essa instância, faz *dumping* de memória, copia os logs para fazer análise forense, disponibiliza para um analista. Tudo isso de forma automatizado, usando um modelo de pipeline e execução de lambdas e processos automatizados.

Então, é importante a gente ter isso em mente, que a nuvem pode nos ajudar, sim, a ter um ambiente tão ou mais seguro usando os recursos que estão disponíveis nativamente. Agradeço o tempo de todos vocês. Deixo aqui meu contato também, para quem quiser me procurar nas plataformas de rede social, enfim, e também meu e-mail da empresa. E agradecer novamente o tempo de vocês e a oportunidade de poder falar com todos. E passo de novo a palavra para a Mesa. Enfatizando que estou honrado de estar aqui com todos vocês, juntos aí para a gente poder bater esse papo. Obrigado.

SR. EDUARDO BARASAL MORALES: Obrigado, Marcello. Muito interessante tudo o que você explanou aí sobre a questão de cloud. Bom, pessoal, não terminou a live ainda, a gente vai agora para a parte

de perguntas. Então se você ainda está com alguma dúvida em cima de alguma das apresentações, fica à vontade para escrever aí no chat que a gente está coletando essas perguntas e agora a gente vai ler elas para nossos painelistas, tá?

A primeira pergunta que veio para a gente é do Diego: *"Qual a opinião de vocês sobre a necessidade e importância de proatividades no CSIRT? Vejo, talvez, pelo termo 'resposta a incidentes' o entendimento de que estes grupos atuariam apenas de forma reativa."* E aí eu gostaria de chamar a Lucimara para falar sobre essa pergunta. Lucimara, fica à vontade.

SRA. LUCIMARA DESIDERÁ: Bom, é verdade, o nome "resposta a incidente" lembra muito reatividade. Mas o CSIRT, ele pode ter, sim, um papel bastante importante na prevenção de incidentes. E principalmente ter atividades proativas na área de gestão de incidente. A gente amplia um pouquinho e fala mais da gestão do incidente, não só a resposta, ao tratamento e à resposta de incidentes. Então, sim, existe, é muito importante que o CSIRT faça isso. Óbvio, isso depende muito de como a sua organização define aí os serviços do CSIRT, né, de como o CSIRT é organizado, é estruturado. Porque em organizações muito grandes, eventualmente, esse papel é feito por outras áreas dentro da empresa. Mas se vocês olharem lá naquele framework que eu comentei com vocês, o framework de serviços de CSIRTs que o FIRST desenvolveu, tem, sim, serviços que são muito... serviços que querem dizer proativos, né? Então a gente tem lá a parte de consciência situacional, onde você tem toda parte de *threat hunting*, que envolve também a parte de você ter medições na rede, tenta entender... ter os *honeypots*, por exemplo, como a gente tem aqui no CERT.br. Então tudo isso são serviços que tentam entender a situação e tentam ajudar a prevenir, a você ser mais preventivo nas ações, tá?

Enfim, sim. Na minha opinião, é importante, mas é óbvio, isso vai depender de como a atual organização quer estruturar os serviços do CSIRT, tá? Se alguém mais quiser complementar, quiser falar alguma coisa, está aberto.

SR. EDUARDO BARASAL MORALES: Alexandre, quer complementar?

SR. ALEXANDRE BERTO NOGUEIRA: Sim. Eu acredito que seja essencial nós estarmos colocando de uma forma preventiva esse nosso trabalho. A pergunta que fica é: qual o tamanho da sua equipe? Qual é o escopo que ela vai ter? Qual é a comunicação que ela vai ter com, por exemplo, uma possível equipe de redes? Então isso tudo tem que estar muito bem azeitado. Você tem que ter muito bem definido esses canais, porque eles são muito usados, né? Você precisa da equipe de redes para ter uma ação rápida. Se você descobre algo, você

precisa agir de forma rápida. E, se você não tem autoridade ou meios para agir na rede, você vai precisar da equipe de redes para atuar.

E também você vai precisar de ferramental. O que você vai utilizar? É aquela expressão que nós estávamos comentando do *hit first*, ou seja, você procurar atingir o adversário, ou o inimigo ou o malicioso primeiramente, antes de ser atingido, então você vai ter que ter um ferramental. Você vai utilizar flows? Por exemplo, a Unicamp, ela tem uma experiência de estar utilizando flows e buscar se o nosso tráfego está conversando com endereçamentos de botnets. E isso é uma proatividade. Se algum endereçamento nosso está minerando criptomoedas. E isso é uma proatividade, porque muitas vezes pode indicar algo está ocorrendo naquela máquina também. Então você tem que ter [ininteligível] a necessidade com a comunicação rápida e dinâmica e também com o ferramental próprio, tá certo, para que você possa colocar não só esse desejo de proatividade, como uma efetiva proatividade, tá certo?

SR. EDUARDO BARASAL MORALES: Ricardo, gostaria de complementar?

SR. RICARDO KLÉBER: Opa. Um detalhe importante, pessoal. Achei muito boa essa pergunta do Diego, porque nós temos, na área de informática, diversos termos que foram cunhados, foram produzidos em uma realidade, e depois essa realidade mudou, e os termos ficaram. Vejam aí que... por exemplo, IDS, sistema de detecção de intrusão, *intrusion detection system*, mas só que a gente sabe, pelo menos quem implementa IDS, que IDS, hoje, se pudéssemos refazer esse termo, seria o sistema de detecção de incidentes. Porque muito incidente detectado pelo IDS não é uma intrusão, mas ficou *intrusion detection system*. Então vamos lá para o contexto do início de CSIRTs, havia uma demanda crescente por especialização em tratamento a incidentes de segurança. Isso, porque como muitos colocaram aí no chat, todo mundo fazia, e ainda faz praticamente tudo, porque acha que o menino da informática que está ali, ele instala o Windows, bota cabo, atende o telefone e vai lá tratar incidentes. O que se precisava no momento em que se criou esse termo era que tivesse uma equipe dedicada a apagar incêndio de forma normatizada. Esse é contexto de 25 anos atrás. Hoje, se pudéssemos refazer o termo CSIRT, com certeza traríamos não só a resposta a incidente, como também o tratamento e manutenção de sistemas para essa equipe e, claro, essa política de proatividade, que envolve a prevenção, a manutenção e o tratamento de incidentes. Acho que é questão histórica aí, mas não dá para recunhar o termo.

SR. EDUARDO BARASAL MORALES: Lucimara, quer fechar a pergunta?

SRA. LUCIMARA DESIDERÁ: É bem isso, né? Historicamente, o termo começou assim, mas a evolução nos mostra que prevenção, ela é fundamental. E o papel do CSIRT é muito importante nisso, né? Um outro elemento que também faz parte aí da parte de prevenção e que a gente trabalha muito aqui no CERT é a parte de conscientização, né? Então a parte de transferência de conhecimento. Então, ajudar as pessoas, treinar as pessoas, trazer conhecimento, trazer entendimento dos problemas, dos riscos e como se prevenir, isso também é um papel que os CSIRTs podem fazer e que tem a ver com a prevenção, né, dos incidentes para evitar que eles aconteçam antes de ser só um mecanismo de responder a incidentes. Assim como os próprios bombeiros, né? O bombeiro apaga incêndio? Apaga. Mas os bombeiros também têm um papel de prevenção e de conscientização no sentido de como evitar que os incêndios ocorram. Então acho que é bem isso, é fundamental, sim, o papel do CSIRT na prevenção e na proatividade para evitar incidentes. Próxima pergunta.

SR. ANTONIO MARCOS MOREIRAS: Bom, obrigado a vocês aí pela resposta nessa primeira pergunta. Eu quero trazer uma pergunta também do Diego aqui. Aliás, Diego, obrigado pelas excelentes perguntas aí. E emendar uma pergunta também aqui do Paschoal Diniz, né? Então, a pergunta do Diego é o seguinte: *"Qual a opinião de vocês sobre a importância do escopo do CSIRT? CSIRT cuida de firewall? SOC, aplica patch?*". E a pergunta do Paschoal Diniz é a seguinte: *"Vocês seguem algum framework de gestão de incidentes, algum padrão de fluxo de processo? Como funciona essa classificação de incidentes?*". E daí eu tentando aqui generalizar um pouquinho, o nosso público, tem muita gente aqui de provedor, e a gente provedor de diversos tamanhos, e às vezes o cara do provedor parece esse cara que o Ricardo Kléber estava comentando agora há pouco, é o cara da informática que faz tudo. Instala o sistema operacional, configura roteador, implementa RPKI, vende para o cliente, atende telefone, faz o cafezinho, manda fatura. O cara do provedor, em alguns provedores, provedor pequenininho, a pessoa faz tudo. Então a minha pergunta, dentro dessa questão de definir melhor o escopo do CSIRT é a seguinte: dá para misturar? O CSIRT tem que ser uma equipe especifica para cuidar de tratamento de incidentes, ou pode ser um a função de alguém que também tem outras funções dentro do provedor? Dá para misturar isso? Não dá? É mais uma questão de ter uma equipe ou de ter um processo de tratamento de incidentes? Como é isso? Gostaria de direcionar essa pergunta primeiramente, porque as perguntas foram direcionadas pelo pessoal do chat para ele, para o Alexandre. Depois, se alguém quiser comentar dos outros palestrantes, também fique à vontade. Alexandre, você poderia falar um pouquinho?

SR. ALEXANDRE BERTO NOGUEIRA: Bom, vamos lá. A questão de escopo vai dizer muito sobre o tamanho, claro, do tamanho

da rede, quantas pessoas eu tenho e quanto tempo de dedicação eu tenho para me envolver com a parte de segurança. Bom, se você é um autônomo system, e acredito que a primeira coisa que você deve pensar é como que, por exemplo, outras organizações vão ver a minha segurança. Então a primeira coisa é você pensar em ter um contato, contato válido aí. Ou seja, outras pessoas, outras instituições vão querer conversar com você com algum problema que esteja saindo, você vai ter que ter um contato válido e funcional. Alguém que esteja lendo aquilo e atuando em cima de algum problema.

Bom, se você quer, se você tem uma organização grande, é claro que você não vai poder ter tanta flexibilidade para atuar em várias áreas ao mesmo tempo. Mas é importante que você tenha um tempo que você se dedique àquele trabalho da parte de segurança. Alguém tem que ler aquele e-mail. De repente, o CSIRT está mandando todo dia algum DDoS saindo da sua rede, e você não está sabendo, e você não está agindo, porque você não tem aquele contato válido. Então o escopo vai dizer muito sobre a quantidade de pessoas e a quantidade de tempo que é definido para aquela pessoa poder atuar, certo? [ininteligível] da Unicamp, nós temos mais de 20 mil funcionários, alunos, tudo mais, é impossível você repartir a tarefa de quatro analistas de segurança com funções de rede. Não tem como. Então vai dizer, o que vai dizer é o tamanho da rede que você vai poder... que você tem atribuído a você, tá certo?

Bom, quanto ao escopo, né? É a mesma coisa. Eu vou só responder incidente? Eu vou analisar malware? Se eu estou dividindo as minhas atenções não só com segurança, mas com outras coisas, você vai ter que definir sua propriedade. Então, por exemplo, resposta a incidente talvez nesse momento se torne mais rápida e prioritária do que fazer uma análise de malware, tá certo? Então, a pergunta sobre deve ou não deve é muito perigosa da gente falar, mas vai depender de acordo com o escopo e a quantidade de pessoas que estão atuando naquele momento.

Sobre a questão de processos, muito ajuda quando você define os processos da sua organização de segurança, por que eu falo isso? Temos vários frameworks que estão disponíveis, a Lucimara trouxe alguns, alguns exemplos, o próprio Ricardo falou de outros, mas quando trazemos para o nosso ambiente, a gente pode receber um impacto e falar: Opa, aquilo não se encaixa totalmente no meu ambiente. Então aí é momento de você fazer desenhos do processo, seguindo o modelo daquilo que você tem e você desenhar o que é um incidente de segurança para você, o que é um ataque DDoS, como você vai atuar, como você vai encaixar ele e fazer toda a classificação dele na sua infraestrutura e como você vai guardar isso para momentos futuros, entendeu? Então a questão de processo, ela vai te agilizar bastante. E você tem uma ferramenta que faça essa análise de

processos, receba essas informações e ela catalogue de acordo com o que você definiu. Por exemplo, antigamente, o Cert vai se lembrar, antigamente era muito no ambiente Asc(F), né? Editando e-mails, fazendo construção dos e-mails, muita coisa manual, e isso toma tempo. Uma ferramenta de catalogação de tíquetes, controle de tíquetes, vai facilitar bastante para você. Não acho que, por exemplo, você tenha que tornar tudo automatizado. Bateu, está batendo um certo tipo de tráfego e você deixa uma ferramenta tomar a decisão de bloquear ou não? Isso pode se tornar um problema para você. Então, o olhar humano ainda é necessário, mas algumas ferramentas podem tornar a vida nossa, poupar muito tempo nosso no dia a dia. A segunda questão, Moreiras? A segunda questão era?

SR. ANTONIO MARCOS MOREIRAS: Era sobre os processos, né? Era sobre se tem algum framework de processos específico ou algo do gênero, tem?

SR. ALEXANDRE BERTO NOGUEIRA: Olha, por exemplo, nós não seguimos nenhum processo. Eu cheguei depois, já definidos os processos, mas muito do que ajudou foi a questão de capacitação com o Cert. Isso nos ajudou a construir os processos, e a gente segue esses procedimentos para catalogação do nosso dia a dia de trabalho, certo?

SR. ANTONIO MARCOS MOREIRAS: A Lucimara acho que tinha citado alguma coisa do Nist, né, Lucimara, que tem um fluxo que podia ser visto aí?

SRA. LUCIMARA DESIDERÁ: Sim, o Nist tem um framework interessante, está sendo bastante utilizado no mercado. E falei, também está sendo recomendado pelo pessoal do comando de defesa cibernética. Lá ele ajuda, vai ajudar a enxergar todos esses passos e dentro do framework três grandes conjuntos de funções lá são tratamento de incidente. Ele é baseado em boas práticas de mercado. Então comece, deem uma olhada no framework do Nist. Inclusive, tinha esquecido de comentar, o framework do Nist está traduzido para português, então tem uma versão em português dele, foi a Câmara de Comércio Americana do Brasil que fez a tradução. Outro material que eu recomendo, além do framework... framework não. É, um framework de serviço do First, perdão. Tem um material que se vocês olharem a minha palestra, eu sempre coloco embaixo as referências, né? Então tem o material da SEI CMU, que é a Universidade de Carnegie Mellon, que foi quem fundou o primeiro Cert no mundo, o primeiro CSIRT no mundo. Eles têm muitos materiais que podem ajudar. Materiais fundamentais que eu recomendo fortemente a leitura, tá? Então na palestra, ela já está disponível, todos os slides têm as referências para os materiais que estou utilizando. Deem uma olhadinha no material do SEI CMU, no material do framework do Nist e o framework de serviços do First. Acho que é um bom começo por aí.

SR. ANTONIO MARCOS MOREIRAS: O Alexandre falou também sobre a importância de ter alguém respondendo e-mail, aquele e-mail de *abuse*, ter o ponto de contato ali. Queria lembrar todo mundo que está assistindo aqui, em particular, o pessoal que é sistema autônomo, que agora faz parte das regras do Lacnic, consequentemente do Registro.br também, a verificação do funcionamento desse e-mail. Então agora para o pessoal que está pedindo um sistema autônomo novo, blocos de IP novos, no processo de solicitação já é feita uma verificação para ver se o e-mail de *abuse* existe, se está sendo lido, se tem respostas coerentes. É um processo que eu acredito que o pessoal do Registro e do Lacnic ainda estejam ajustando, implementando, operacionalizando, de verificação do funcionamento desse e-mail de *abuse* para os processos que... desculpa, me atrapalhei aqui. Para os ASs que já estão alocados, para os blocos que já estão alocados. Então é importante agora, além da função em si de segurança, né? E até porque essa função é superimportante, isso foi colocado nas regrinhas lá, e agora se você não tiver um e-mail de abuse, você está descumprindo as regras de uso do teu bloco IP, do teu Sistema Autônomo. E isso, em última instância, em um caso de gravidade maior, isso pode te levar até a perda do bloco IP ou à perda do Sistema Autônomo, porque você não vai estar mais utilizando ele de acordo com as regras, né? Eu só queria fazer esse comentário aí. Eduardo, você segue?

SR. EDUARDO BARASAL MORALES: Vamos lá, Moreiras. Acho que o Marcello Zillo queria fazer um comentário também sobre as recomendações.

SR. MARCELLO ZILLO NETO: Comentário rápido sobre boas práticas de resposta a eventos, incidentes de segurança, enfim, compartilhei com o time aqui. Provavelmente já vão colocar para vocês no chat. Tem um PDF, que é um guide, sobre processos de resposta, [ininteligível] responde guide para ambientes de nuvem AWS. Desde treinamento, boas práticas, processo, revisitar os processos de recuperação, revisitar processos de resposta, pensar em automação, um guia bem completo. Acho que vale a pena também como referência, especialmente ao usar serviços de nuvem AWS, tá bom?

SR. EDUARDO BARASAL MORALES: Obrigado, Marcello. Bom, seguindo aqui as perguntas. Veio uma do Alexandre [ininteligível] para o Lacier Dias. Lacier, alguns softwares gratuitos para monitoramento de ataque em redes? Fica à vontade.

SR. LACIER DIAS: Então, olha, a gente tem usado bastante o [ininteligível]. Ele usa, auxilia bem, é uma análise de flow que ele faz e reage de acordo com a parametrização que você coloca. Então ele bota recurso em blackhole, ele faz um anúncio para alguma ferramenta externa, e tem algumas APIs. Então, assim, é gratuito, não é deveras

difícil de configurar, é uma ferramenta que eu, que a gente faz uso aqui quando a gente precisa automatizar algumas coisas para alguns clientes.

SR. EDUARDO BARASAL MORALES: Obrigado, Lacier. Alexandre, gostaria de complementar?

SR. ALEXANDRE BERTO NOGUEIRA: Sim, [ininteligível] universidade a questão de recursos, ela é um pouco mais complicada de investimentos em ferramentas, então a gente procura usar bastante as ferramentas de open source, né? Mas, por exemplo, nós estamos tendo bastante experiências boas com, por exemplo, Shadow Server e Shodan, que seriam plataformas aí de visualização da sua rede de uma visão mais externa, né? Então, por exemplo, se você rodar alguma ferramenta internamente na sua rede, ela vai te dar um cenário, mas quando você tem uma ferramenta externa visualizando a sua rede, ou seja, vai ser uma outra perspectiva. Muito interessante, o Shadow Server te envia relatórios: "Você tem portas 23 abertas. Você tem IPs dentro de Blacklists. Você tem serviços que não deveriam estar abertos e estão abertos. Você tem DDoS saindo da sua rede". São ferramentas livres que necessitam de contatos por grupos de segurança então poderiam auxiliar no monitoramento da sua rede. Uma ferramenta de varredura que a gente tem utilizado bastante é o green bone, uma ferramenta aberta, que traz bastante detalhes sobre a visão de inventário e de como está a questão de atualização dos seus dispositivos, não só hosts como servidores mas também dispositivos de rede. Tá certo? Tem os próprios flows de rede, que vão te dar uma visão e você vai ter que fazer ajustes, como o nosso colega falou, de parametrização, aquilo que pode te dar de retorno sobre algum problema que esteja acontecendo. Mas a gente também tem que lembrar que a Team Care tem um serviços [ininteligível] que pode ser bastante útil na questão de você... te auxiliar a verificar se está tendo algum problema na sua rede. Questão de [ininteligível], você direciona flows para [ininteligível] uma ferramenta que ele poder estar te auxiliando, identificando possíveis problemas. [ininteligível]. Então acredito que isso possa ser visto e olhado com cuidado aí, certo? Tudo bem aí? Alô?

SR. ANTONIO MARCOS MOREIRAS: Acho que deu uma falhazinha no áudio aqui, Alexandre.

SR. ALEXANDRE BERTO NOGUEIRA: É? Que parte?

SR. EDUARDO BARASAL MORALES: É, acho que...

[falas sobrepostas]

SR. ALEXANDRE BERTO NOGUEIRA: Está melhor agora?

SR. ANTONIO MARCOS MOREIRAS: Não, está com probleminha no áudio aqui, ainda está um pouquinho ruim. Vamos

fazer o seguinte, deixa eu passar para próxima pergunta aí. Pessoal está brincando aqui que você virou o Robocop, Alexandre. Sua voz ficou bastante forte e diferente. O pessoal estava elogiando agora há pouco a voz do Ricardo Kléber no chat, agora acho que vão elogiar a sua também, Alexandre, que ela é bem marcante, ficou quase Robocop aqui. Deixa eu fazer a próxima pergunta, depois, se você quiser, você volta para complementar, dá uma verificadinha no áudio, enquanto isso. É difícil verificar, porque a gente está ao vivo, você vai verificar áudio, vai acabar saindo no YouTube. Mas tenta dar uma olhadinha se está tudo certo com a conexão à Internet, e a gente te chama de volta aqui.

Eu vou aproveitar e fazer uma pergunta para o Ricardo Kléber. É uma pergunta feita pelo Charles César. Uma pergunta, talvez, um pouquinho menos prática e pragmática, menos a ver com CSIRT, mas ele perguntou assim, ó: "Fechar a Internet em um país como a Rússia, como a Rússia pretende, diminuiria o número de incidentes naquele país?". Então esses países que... a gente vê isso, não é só a Rússia que andou ameaçando fazer isso, não. "A gente não quer mais a Internet global. A gente quer a Internet aqui do nosso cantinho, do nosso país". Um [ininteligível] Garden, quer alguma coisa mais fechada, a China tem alguma coisa assim também, tem outros países que vão nesse sentido. Achei importante trazer a pergunta, porque a gente vê às vezes algumas soluções de segurança, seja nesse escopo global ou em escopos menores que acabam quebrando a Internet, né? Internet é algo global, algo único, se a gente está falando de fragmentar a Internet, a gente não está mais falando de Internet. Mas aqui eu já fiz meu comentário e a minha opinião, queria ouvir mesmo a sua, Ricardo, que a pergunta foi para você.

SR. RICARDO KLÉBER: Tranquilo. Eu vou retomar um pouco aí um contexto de 98, mas finalzinho de 2005, né? Eu acho que alguns aí dos meus alunos que estão on-line sabem que eu era security office da UFRN, o [ininteligível] é dessa época, mudou inclusive até de nome. Mas em 2007 eu vim para o IFRN, deixei de trabalhar, hoje dou só aula, como meus alunos falam. Não estou trabalhando mais, estou só dando aula. Mas, enfim, naquela derradeira ação, última ação ainda na UFRN, antes de sair dessa função de security office, era uma pendenga, uma briga que eu tinha com o superintendente sobre abrir ou não o Sigaa(F), que era o nosso sistema acadêmico, para ser acessado a partir de IPs externos. Por quê? Quem trabalha com segurança quer ter o controle da situação, da sua zona de conforto e acha que estabelecer limites e fronteiras facilita o seu trabalho, mas você restringe uma parcela dos interessados naquele sistema de acessar. E o fato foi que eu saí da UFRN com esse pensamento, e hoje o Sigaa(F) está aberto para todo mundo e não houve problemas em relação a isso. Estou dando essa contextualizada para dizer que essa tentativa de

tentar resolver problema de segurança fechando a sua rede é uma coisa um pouco mesquinha, zona de conforto, mas que não cabe mais. O que eu aprendi, queria compartilhar com vocês, respondendo ao Charles aí, é que quando a gente fala de Internet, veja bem, todas as iniciativas de restrição vão na contramão do movimento natural de evolução da própria rede, da sociedade e da dependência das pessoas e das instituições da Internet. Não cabe. Não cabe. E ainda mais, o fato é que ainda que se alguma instituição, ainda que algum país ou continente queira fazer esse tipo de restrição, existem várias formas de você tentar burlar isso daí. Veja a própria China, o grande firewall da China, que tem VPNs, você tem sistemas que têm amplitude global como o sistema do Elon Musk e Starlink, já que você não pode sair no caminho regular, você vai por outro ponto, faz um túnel, enfim, passa. Mas minha opinião quanto a isso, Charles, e a provocativa mais muito bem colocada aí é que não adianta tentar ir na contramão da evolução da sociedade, das redes. Nós estamos no mundo digital, vivendo às vezes até, e eu tenho medo disso, muito mais no mundo digital do que no mundo real. E em consequência disso e do avanço da tecnologia de apoio ao ser humano e da manutenção aí da sociedade digital, ir na contramão disso é um tiro no pé. É um esforço desnecessário e que pode ser burlado. Não vale a pena, não.

SR. EDUARDO BARASAL MORALES: Obrigado, Ricardo. Bom, seguindo aqui as perguntas, teve uma pergunta do Danilo Lima para o Marcello Zillo: "Qual a garantia que os ataques irão cessar depois de pagar o que o hacker exige? É inteligente confiar no hacker?". Fica à vontade, Marcello.

SR. MARCELLO ZILLO NETO: É, [interrupção no áudio], por outro lado, pode ter qualquer tipo de comportamento. A gente não tem garantia nenhuma. E o que eu costumo sempre dizer é que a recomendação é não pagar. Mas essa é uma decisão muito baseada em risco e tomadas de decisão que às vezes vão muito além da tecnologia. Mas não existe nenhuma garantia, de forma alguma, que isso pode funcionar até na escala que a gente precisa. O que a gente sempre comenta, e acho que todos nós falamos aqui, a importância de ter um plano de recuperação em caso de um ataque muito bem desenhado. Porque se tudo der errado, o seu plano de recuperação tem que ser capaz de voltar o ambiente rapidamente a um mínimo estágio de funcionamento. A minha recomendação, sempre que interagir em casos como esse, não é uma boa prática você, novamente, pagar, porque não vai ter garantia nenhuma e está, na verdade, alimentando isso acontecer de forma mais comum, já que você acaba gerando esse cenário de mercado para isso. Então a recomendação, particularmente, sempre digo: Não pagar. Mas é uma decisão que vai muitas vezes além da TI, da tecnologia, que fica, às vezes, em uma escala muito mais ampla.

SR. EDUARDO BARASAL MORALES: Bem comentado. A gente até tem uma entrevista gravada no Camada8, que é o nosso podcast, com o delegado Alessandro. E a gente comenta bastante sobre esse assunto e de como você fazer uma denúncia, quando sofre aí um ataque cibernético. Então eu já recomendo para aqueles que não ouviram, ouvirem esse episódio aí do Camada8. Lacier, você gostaria de complementar essa pergunta?

SR. LACIER DIAS: Então, isso é uma coisa que a gente recebe, infelizmente, quase toda semana. É um provedor sofrendo ataque, agora o Espírito Santo é a bola da vez, vários provedores do Espírito Santo sendo atacados. E uma coisa que vem acontecendo esse ano: provedores que foram atacados o ano passado e pagaram voltando a ser atacado. Por quê? Porque o hacker... acabou o dinheiro. Ele precisa de mais dinheiro. E se você tendenciosamente pagou, a chance dele te atacar de novo é exponencial. Então, pagar? Nunca. Nunca. em nenhuma condição. É só esse meu comentário, porque muitos provedores pensam em pagar e não têm noção que eles vão entrar para a listinha de pagadores. Então eles vão ser atacados novamente porque pagaram.

SR. MARCELLO ZILLO NETO: Além de tudo, Lacier, questão de implementar os controles corretos, mecanismos.

SR. LACIER DIAS: Ah, sim.

SR. MARCELLO ZILLO NETO: Após um ataque, com certeza, um evento desse tem lessons learning que precisam ser colocadas em prática, né? Senão...

SR. LACIER DIAS: E a grande maioria dos ataques passam por brechas que são, assim, desculpa até a sinceridade, até juvenis. Você olha, e o cara não tem um provedor, ele tem uma peneira. Tinha 20 maneiras de ser atacado. Entendeu? Então, assim, infelizmente essa é a realidade que a gente encontra, não tem uma aplicação de boas práticas, não levam a sério, como deveriam levar. A não ser depois que toma. Aí é o caso do cara que foi assaltado, depois ele compra um carro blindado, ele quer botar cerca elétrica, quer botar concertina, quer blindar a casa dele inteira. Entendeu? Mas depois que já aconteceu. Acho que tem que trabalhar preventivamente. A gente com relação a preventivo no Brasil ainda tem uma estrada para caminhar.

SR. ANTONIO MARCOS MOREIRAS: Legal, gente. É, obrigado aí por todas as perguntas, por todas as respostas. Eu vou chamar agora os palestrantes, na mesma ordem das palestras aí, das apresentações para fazer os comentários finais. Mas, antes disso, aproveitar atenção de vocês aí, em primeiro lugar, queria perguntar para a equipe: vocês conseguem colocar no YouTube aí o QR Code já com nosso questionário de avaliação? Porque é bastante importante. Não estou mandando ninguém embora ainda, pessoal. Pessoal ainda vai fazer os

comentários finais, temos resultados dos sorteios e várias coisas aqui ainda nos próximos minutinhos. Aí, o QR Code já está no YouTube. Apontem aí o celular, ou peguem, vai estar no chat também o link para avaliação. São só duas questões. É uma nota que você dá lá de zero a dez, para dizer se foi boa ou não. E coloca o ponto que acha mais importante que a gente saiba. Pode ser algum aspecto que a gente tenha que melhorar para a próxima live, pode ser algum elogio ou algo que você achou muito legal. Então faça isso daí. Certo?

É, bom, um outro ponto que eu gostaria de lembrar a vocês ainda, antes de passar a palavra para a Lucimara, enquanto vocês vão respondendo à pesquisa. Nós vamos ter esse ano o IX Fórum e a Semana de Infraestrutura presenciais, em São Paulo. Aquele evento tradicional que o NIC.br promove, grandão. Tem o GTR, o GTS e o IX Fórum. IX Fórum vai ter três dias de duração, de 26 a 28 de outubro de 2022. Essa semana inteira, de 26 a 28, tem a Semana de Infraestrutura, né? Junta também o GTS e o GTR. Anotem na agenda, se programem para vir para São Paulo. É um evento superinteressante. Evento que sempre tem palestras, muitos palestrantes internacionais, tem tradução simultânea, português, inglês, espanhol. Ele é transmitido, mas é muito diferente você estar aqui presencialmente em um evento. Aqui não, porque não estou em São Paulo hoje. Mas você estar presencialmente no evento participando. Então se vocês puderem, se programem. E nessa sexta-feira agora é o último dia para mandar proposta de apresentação. Então quem tiver alguma palestra interessante, algum tema interessante, alguma proposta de painel, proposta de apresentação, é agora nessa quinta-feira, nessa quinta-feira... nessa sexta-feira, dia 15/7 o prazo final para mandarem para a gente, para a gente colocar no programa. Então convido aí todos os palestrantes aqui a mandarem suas propostas e vocês que estão assistindo a live e que têm temas interessantes para serem tratados para que mandem suas propostas. Vamos lá. Vou chamar todo mundo aqui para a rodada final de comentários finais e fechamento do nosso evento. Lucimara, você pode ser a primeira?

SRA. LUCIMARA DESIDERÁ: Vamos lá. Não vou me alongar muito, porque o material está aí, links aí, vocês podem ver a parte do framework, o que é definir o CSIRT, atividades e tudo mais. Uma coisa que todo mundo falou, atividades de um CSIRT dependem muito do tamanho da sua rede e tamanho da tua operação. Gostaria de reforçar coisas que Ricardo Kléber falou e que Alexandre falaram, o CSIRT, primeira coisa, ele é o ponto de contato. E o próprio Moreiras também falou isso, da questão de alocação de um ponto de contato agora para os recursos de AS. Em primeira instância, primeira coisa que um time de resposta em incidente é o ponto de contato. Então, estruturem suas operações, suas operações, seus processos, entendam o que é resposta de incidente, vejam links que a gente mandou e definam o

seu ponto de contato. A primeira coisa a pensar é: o CSIRT é um ponto de contato para tratamento de incidentes, tanto para os seus incidentes como para os que ocorrem com outras instituições e que elas podem precisar do seu apoio para conseguir resolver. Primeira coisa: CSIRT é um ponto de contato. Obrigada.

SR. ALEXANDRE BERTO NOGUEIRA: Será que o áudio agora está bom?

SR. ANTONIO MARCOS MOREIRAS: Sim, Alexandre. Está ótimo.

SR. ALEXANDRE BERTO NOGUEIRA: Invista na visão da sua rede, seja com flows de rede, ferramentas de monitoramento, invista em você ter uma visão, invista em você descobrir se você tem pontos cegos na sua instituição. Invista você ter algum parceiro, como se fosse um, por exemplo, Shadow Server que avalie se de fora tem algum serviço que esteja no ar que você não esteja sabendo, mas faça o trabalho de casa. Invista na visão de rede, em flows de rede. Estamos aí para estar ajudando. Se precisar de algum trabalho com scripts, tal, como vocês viram, é uma plataforma que não dispende muito de recursos e pode ser muito útil para vocês. Evitar não só ter proatividade em algum problema mas também trabalhar, caso ocorra algum incidente de segurança, ou quando ocorrer o incidente de segurança, você poder correlacionar todo esse tráfego, todos endereços que bateram no seu ambiente aí.

SR. ANTONIO MARCOS MOREIRAS: Ricardo Kléber.

SR. RICARDO KLÉBER: Bom, finalizando aqui. Reforçar os três pontos principais ali, se a gente pode resumir aí a fala ou a participação em três palavras, são as três palavras que a gente colocou no slide 3: proatividade, cooperação e capacitação. Sem dúvida, proatividade acho que todos falaram isso. Hoje não tem mais como você trabalhar só apagando incêndio, e o foco, acho que todo mundo saiu daqui com essa percepção, quem não tinha, de que precisamos avançar, ir além daquela coisa de ficar aguardando, sair da zona de conforto. Não existe mais. Segundo, a questão da cooperação. Todo mundo quer cooperar, mas na hora em que é vítima do incidente, às vezes, fica aquela coisa, não vou expor minha empresa, não vou expor minha instituição, quero resolver sozinho. Dependendo do tipo de ataque, você vai falhar. Procure cooperação, o Cert está aí, os eventos do First, eventos [ininteligível] estão aí para ajudar nesse processo. E finalmente a questão da capacitação. Tem que estar atualizado não só nas tecnologias mas também no ferramental e nas metodologias normativas de resposta a incidente de segurança e criações do CSIRT. Estamos à disposição. Mais uma vez, obrigado pelo convite e qualquer coisa nossos contatos estão aí nos slides. Valeu, pessoal, abraço, até a próxima.

SR. ANTONIO MARCOS MOREIRAS: Lacier.

SR. LACIER DIAS: Pessoal, a gente sempre enfatiza que dê a devida atenção antecipadamente à segurança, mas se você fizer o mínimo já vai estar anos-luz à frente. Costumo comparar comportamento de segurança com estouro de manada. Em 10.000 provedores, pouco mais, pouco menos no Brasil, seu provedor tem que ser o que está na frente da manada, porque o leão vai correr atrás de você, vai correr atrás da manada e vai pegar alguém. Porque a gente aqui trabalha em prol da segurança, mas a gente não pega bandido. Quem pega bandido é polícia. A gente ajuda, indica, gera log, gera evidência, tal, municia, mas prender, quem prende é a polícia. Você tem que ser o que está na frente da manada, porque se for o que está atrás, o leão vai te pegar. Fica a dica aí.

SR. ANTONIO MARCOS MOREIRAS: Marcello, seus comentários finais.

SR. MARCELLO ZILLO NETO: Primeiro, um agradecimento, novamente, pelo convite, foi um prazer estar aqui com vocês. E acho que gosto sempre de enfatizar que no caso de ambientes de nuvem, usem a nuvem para você ter mais agilidade também no processo de resposta, tem recursos nativos. Então se eu pudesse pedir três coisas aqui: primeiro, cuide da identidade, a gente falou disso. Identidade digital é o novo ativo que usuários mal-intencionados querem. Use NFA, como a gente falou. Segundo, questão de logs, trilha de auditoria. Garanta que você tenha esses logs e que eles são utilizados da melhor forma possível. E, também, utilize automação, segurança como código para escalar. Porque na medida em que as empresas vão adotando mais tecnologia, nós, em segurança, a gente passa a ter um desafio também ,que é como é que a gente põe segurança em tudo isso ao mesmo tempo. Então dá para usar security by design usando APIs e recursos nativos que estão disponíveis na nuvem. De novo, obrigado a todos. Foi um prazer estar aqui com vocês.

SR. ANTONIO MARCOS MOREIRAS: Eu quero agradecer a todos vocês aí, Lucimara, Alexandre, ao Lacier, ao Ricardo, ao Marcello, por terem aceitado nosso convite, por terem participado da live e feito essas apresentações e todos esses comentários aí brilhantes e muito elucidativos e educativos para nossa comunidade técnica. Eduardo, você segue?

SR. EDUARDO BARASAL MORALES: Sigo. Agradecer a todos que estão vendo e ouvindo até agora. Além de agradecer os palestrantes, gostaria de agradecer todo mundo que está nos acompanhando no YouTube e Facebook. Bom, queria dar nossos últimos avisos. São nossos cursos, nossos eventos. Então a gente vai ter o IX Fórum Regional de Caruaru, que é dia 29/7, as inscrições estão abertas, a grade já está montada. Para você que é do Nordeste, pode

se inscrever e participar lá com a gente. Vamos também ter um curso BCOP a distância, para você estudar a distância, da sua casa, do conforto do seu lar. Inscrições também estão abertas até dia 17/7. Quem quiser pode se inscrever no link que está sendo colocado no chat. Temos também a próxima Intra Rede, né? Que é sobre ferramentas para operação de redes. Então quem quiser, pessoal, já fica atento, que no dia 10/8 a gente vai ter nossa próxima live Intra Rede. Teremos também o curso BCOP em Belo Horizonte, que vai acontecer do dia 22 a 26/8. Nosso último curso BCOP presencial que vai acontecer, e as inscrições também estão abertas, quem quiser pode se inscrever. E temos aí também o curso do NetAcad, que é o Switching, Routing, and Wireless Essentials. Quem quiser se inscrever nesse módulo pode. A gente está terminando de gravar o módulo 3, em breve deve lançar o módulo 3 do CCNA. Então fica atento aos nossos anúncios. E temos também alguns outros cursos em parceria com a Cisco, como o de cibersegurança essencial, introdução a cibersegurança, que acabam sendo muito parecidos com o que a gente já disse na nossa live. Então temos também de introdução a Internet das Coisas. Quem quiser pode se inscrever. Tá? O que mais de avisos a gente tem?

Bom, a gente tem que falar os ganhadores, né? Então aqui a gente tem o kit NIC, quem ganhou foi a Valderlei Yasmim Arruda Silveira. Kit NIC junto com todos nossos patrocinadores que mandaram um brindezinho. Temos dos kits extras, né? Voucher da Super Conhecimento, mais o voucher de desconto da Solintel/VLSM, são quatro que foram sorteados, quem ganhou foi : Floriano de Souza, Lucas Martines, Sérgio Luís Fava e Ricardo Ferraro de Souza. Então pessoal está colocando no chat, depois eles vão entrar em contato. E temos também os sorteios dos patrocinadores, né? Que no caso aqui da Globo, né? Que é o voucher da Globoplay lá por dois meses, que é o Levi Silva Souza. E temos também da 4Linux, que é um curso à escolha do ganhador, que quem ganhou foi o Hugo Nascimento.

Por fim, também gostaria de falar que a gente vai ter a Semana de Capacitação, que é uma semana de tutoriais que vai acontecer do dia 12 ao 16 do mês 9. Então fica atento. O Camada8, a gente já comentou, está saindo um episódio hoje, então fica atento que a gente deve lançar daqui a pouquinho um novo episódio. A gente faz mensal o projeto. Temos o curso IPv6 a distância, que você pode fazer no seu tempo, pode se inscrever. E temos também o curso IPv6 avançado presencial, que é a nossa última turma do ano, que vai acontecer aqui em São Paulo. Inscrições vão até dia 28/8, tá, pessoal? Vários cursos para você especializar e melhorar o seu currículo.

Por fim, gostaria de agradecer aos nossos patrocinadores, que são: Dattas Link IP, Servidores e Datacenter, FiberX, Globo, Icann, Netflix, 4Linux, Solintel/VLSM, Cisco, Super Conhecimento, com apoio

de mídia da Revista RTI, Infra News Telecom e Editora Novatec, tá? Então esses daí são nossos patrocinadores aí que nos ajudam na live. Temos também o código de desconto da Novatec Editora, pessoal vai colocar no chat, que é Intra Rede, tudo minúsculo, você ganha uma porcentagem dos livros comprados no site deles.

Por fim, antes da gente terminar, eu queria dizer que a gente anotou todas as perguntas, agora a gente vai passar as perguntas para os palestrantes, aquelas que não foram ditas aqui durante a live. E eles vão, depois, nos mandar respostas, ou vão colocar nos comentários dos vídeos. Tá? Então depois que terminar a live, lembra de voltar no vídeo para dar uma lida lá na sua pergunta, de como ela foi respondida. Isso daí deve acontecer ao longo dos dias, tudo bem? Gostaria agora de chamar, então, vídeozinho do Cidadão na Rede. Pode tocar.

[exibição de vídeo]

SR. ANTONIO MARCOS MOREIRAS: Quero agradecer muito a participação de todos. Antes de terminar aqui, mais um recadinho ainda. Pessoal de Salvador, pessoal da Bahia e região, no dia 27 e 28, agora desse mês, finalzinho, daqui a duas semanas, eu vou estar por aí num evento chamado atualiza Telecom, falando do OpenCDN. A gente tem muitas novidades no OpenCDN aí que está no PTT de Salvador. Então teve redução de valor, lá no OpenCDN, tem várias CDNs já participando, então é algo que se vocês não conhecem, vale a pena conhecer. Podem procurar a gente a qualquer hora. Podem ir procurar a gente presencialmente nesse evento que vai ter aí na capital da Bahia. Pessoal de Brasília também, de Goiás, de Goiânia, outras regiões próximas aí, sei lá, sudoeste, é, sudoeste de Minas, que estão próximos ao PTT do Distrito Federal, PTT de Brasília, também fiquem atentos ao OpenCDN e ao próprio PTT de Brasília. Nós já estamos lá com OpenCDN operando com uma CDN, tem CDNs novas que vão chegar até o final do ano. Já tem o valor definido. E a gente está aceitando as adesões ao OpenCDN lá no PTT de Brasília.

Bom, depois desses recadinhos finais aqui, agradeço novamente todo mundo que participou. Vocês que participaram fazendo perguntas, comentários excelentes no chat. Todos nossos painelistas, palestrantes aqui de hoje, todos os patrocinadores, toda a equipe interna do NIC.br que fez esse evento ser possível. Agradeço a todos e ficamos por aqui hoje. Obrigado.