DURBAN - GAC Encontro com SSAC
Terça - feira, 16 julho, 2013 - 9:00-10:00
ICANN - Durban, África do Sul

HEATHER: Bom dia para todos. Por favor vão sentando. Hoje de manhã o GAC vai ter uma troca de opiniões com o comité de segurança e estabilidade, que vai apresentar o que nós consideramos os temas mais importantes que queremos receber informação a atividade do SSAC, queremos aproveitar o máximo possível, no curto tempo que temos, nesta reunião com o SSAC. Então sem outra demora eu passo a palavra á Patrick Faltstrom, que é o Presidente do Comité que assessora a estabilidade e segurança.

PATRIK FALTSTROM: Obrigado Heather. Obrigado a todos os membros do GAC. Que dão a oportunidade de nos reunirmos. Eu sou o Presidente do Comité Assessor de Segurança e estabilidade da ICANN, à minha direita Jim Galvin, o vice-presidente. O SSAC começou em 2001, começou os seus trabalhos em 2002, somos um comité assessor, da mesma forma que o GAC, ao qual vocês pertencem. A nossa carta de organização inclui o requerimento de assessorar o conselho e assuntos referidos sem ser a segurança e estabilidade do sistema de atribuição de nomes e endereços de internet. Os nossos membros têm um membro de uma duração de 3 anos no cargo, e já que temos pouco tempo e vocês também têm material recebido e enviado antes por nós, vou parar por aqui vou perguntar aos membros do GAC se têm alguma pergunta

especifica a respeito das nossas operações. Eu não vejo perguntas, então eu vou pedir que seja apresentada aqui na tela os *slides* a respeito do certificado de nomes internos. Este é o número de documento 57 e a forma em que nós produzimos documentos é através de grupos de trabalhos que chamamos "corpos de trabalho" e cada um trabalha em assuntos que depois podem produzir um relatório. Um documento quando há consenso a respeito desses corpos se apresentam um documento e depois é publicado, e disponibilizado. É possível que os membros do SSAC pedir que se incorpora alguma objeção ao documento, isso já aconteceu em outras vezes. Mas geralmente no SSAC conseguimos trabalhar com consenso para emitir um documento. Esse é um desses documentos no qual atingimos consenso. Esse assessoramento específico identifica que uma autoridade de certificação, ou de habilitação, emite certificados de comunicação e segurança. Especialmente para as páginas web e outros protocolos. Acontece que essa prática da autoridade de habilitação e muito utilizada e pode ser um risco para a integridade das comunicações seguras através da internet. Essa prática pode ter impacto dos novos GTLDs. Neste relatório recomendamos que a ICANN tome medidas imediatas para mitigar esses riscos. Esse relatório foi acabado no começo do meio de janeiro deste ano. O próximo *slide*, por favor. Assumimos esse relatório e apresentamos á ICANN e depois do assessoramento desse SSAC, a ICANN tomou ações de mitigação imediatas para reduzir o risco. No entanto, ficam ainda alguns riscos residuais e temos que trabalhar muito mais para resolver esses riscos. O seguinte *slide*, por favor. De forma resumida, o que esse relatório trata é o seguinte. Houve, existia uma prática entre as autoridades de certificação de emitir certificados na medida que não existem no DNS,

esse relatório descreve o que acontece se for o caso que os certificados que são entregues para nomes de domínios, que ainda não estão na zona raiz, depois são delegados no processo dos novos TLDs. A explicação técnica do que acontece a de que se existe um certificado para o nome de domínio, que quando nome de domínio é delegado, depois como …, cobre um serviço, é segura a conexão ao serviço para o qual o certificado não foi emitido. Há muitas pessoas nesta sala, aqui, sem dúvida não vão ter problemas em discutir esse problema. Se SSAC, é a mitigação que a ICANN emitiu for de colaboração e comunicação com CA *browser*, que é a organização de certificação e fornecedora de browsers para produzir políticas a respeito de como agir e mudar as práticas, para minimizar o risco. Perguntas a respeito?

HEATHER: Muito obrigado Patrick. Reino Unido

REINO UNIDO: Comentário adicional, qual é a escala de utilização de uso por parte das empresas e serviços internos que cria este conflito. Estamos a falar de centenas, milhares de empresas, de quanto? Vai existir um impacto no mundo empresarial quanto se tentar corrigir?

PATRIK FALTSTROM: Há duas respostas. O relatório foi disponibilizado no prazo de Janeiro a Março, por isso eu não me lembro do número exato. Então sugiro que por favor dê uma olhada no relatório para que não falhe uma coisa que não é exatamente verdade. A razão pela qual nós emitimos este relatório, porque o uso é bastante estendido. Posso concluir que

também esses métodos de mitigação, possivelmente só vêm o problema dentro do possível. Seja ou não um problema inerente á própria tecnologia que está a ser utilizada. Isso significa que novos não poderão melhorar muito mais. O risco continua existindo por isso, digo, que esperar ou demorar a introdução de TLDs, não necessariamente irá ajudar. Agora talvez. Á uma pergunta que tem a ver com o aspeto um pouco diferente. O que acontece se uma empresa, uma companhia, esta utilizando para qualquer propósito um nome de domínio que hoje em dia não existe na internet, mas depois sim vai ser delegado. Então isto é uma coisa que nós não analisamos no SSAC e o conselho solicitou fazer um estudo a respeito de problemas de colisão. Vocês deveriam ler os certificados, relatórios e certificados internos, como um exemplo destes temas de colisão. E a pergunta é de que, que acontece se delegada um nome de domínio que está sendo utilizado numa empresa. Ai sim então vai existir um impacto por várias razões técnicas. Como a rota de busca e outros elementos. Mas a ICANN pediu um estudo através do conselho e num relatório prévio, acho com o número 45, analisa esses problemas de colisão de nomes. Também para ver até que ponto que risco existe para por esses problemas de colisão de espaços de nomes.

HEATHER: Agradeço Patrick. Eu acho que está depois Malásia e Países Baixos.

MALÁSIA: Obrigado. Eu sou da Malásia. Eu tenho uma pergunta. Talvez já foi respondida. De todas as formas eu gostaria que me explicassem um pouco melhor porque o impacto no usuário final, com essas autoridades

de certificação. O que acontece com eles? Obrigado.

PATRIK FALTSTROM: O impacto para o usuário final do certificado pode acontecer é que o usuário final se conecte, por exemplo, com *web browser*, um sitio *web*, um a pagina *web*, e veja que o cadeado está fechado e considere que á uma comunicação confiável. Mas na verdade a conexão não é para o sítio, ou pagina web ou web site que ele está querendo mas para outro. Isso é o que pode acontecer com a pessoa. Motivo pelo qual nós, no SSAC, dizemos que ainda existem riscos, na não obstante a mitigação é que é muitos mecanismos de ataque, que podem enganar os usuários finais de que a comunicação é segura. Então eu diria, para responder à sua pergunta, é que não. Não avaliamos esse risco, a comparação de outros.

HEATHER: Países Baixos por favor.

PAÍSES BAIXOS: Obrigado Patrick pela apresentação. Eu quero fazer uma pergunta. Que esperam vocês do GAC? Eu acho que o SSAC, eu acho que já colocou o olho neste ponto e está analisando o que tem a ver com comunicação. Ou seja disse que a ICANN implementou ações. Que espera do GAC?

PATRIK FALTSTROM: Eu não tenho espectativas específicas do GAC eu tenho expectativas de toda a comunidade da ICANN, de obviamente está incluído o GAC. Os problemas de coleção de nomes e espaços de nomes é um problema

sério. E é uma coisa que já foi assinalada em outros documentos. O que fizemos nesse SSAC, no documento 45 de 15 de novembro de 2010 e 57 de 27 de março, que é esse documento referido á certificado de documentos internos. Se há outros documentos também, o que está acontecendo neste momento é que a ICANN fez uma pesquisa para ver quais os riscos reais de colisão de nomes reais. Se este estudo, essa pesquisa, pelo que eu entendo, está quase a finalizar para se apresentado à ICANN. E nós, e bem como outros grupos, estamos esperando os resultados dessa pesquisa, conclusões, baseadas no relatório. E nós no SSAC o que pediu, o conselho especificamente, e que fizéssemos uma explicação, ou umas sugestões, a respeito de mudanças neste relatório. O que eu penso a nível pessoal, é que nós vamos ver algum tipo de período de comentários públicos, quando aos achados. Então ei quero que inclusive o GAC, mantenha os ouvidos alerta para esses comentários. Se é que o GAC considera necessário, Nós no SSAC pediram que nós devemos estar alerta e esperamos que as conclusões e as pesquisas sejam feitas de uma forma solida, no ponto de vista de segurança e estabilidade. Que eu, que nós, estamos interessados.

HEATHER. Depois Sri Lanka.

SRI LANKA: Obrigado Senhora Presidente. Bom dia. Sou Jayantha Fernando de Sri Lanka. Em primeiro lugar queria agradecer a Patrick pelo excelente trabalho que estão realizando nesse âmbito, Tenho um comentário breve e uma sugestão. Embora tenhamos sido um dos primeiros códigos de pais em estar em DNSSEC e operando nesse ambiente, vemos que

muitas organizações de muitos bancos, também nos sistemas de nomes de domínio, e queríamos, e vimos também como se construi esse ambiente de CA. Queremos criar uma cooperação, há alguma maneira de, que as expressões que fosses fizeram possam implementar-se e alimentar o CAs que operam? Nos âmbitos dos países em desenvolvimento e de alguma maneira de que o GAC possa dar uma plataforma através da qual se possa espalhar essa informação para as autoridades, queria saber qual a sua opinião?

PATRIK FALTSTROM: Como eu disse antes e SSAC, também apontamos no nosso relatório certificados de nomes internos, que não vemos uma solução plena, a questão dos certificados se continuarmos utilizando certificados da maneira que estivemos até ao momento. Com a lista de autoridades de certificação confiáveis. O que dizemos é que uma maneira de avançar é que em lugar de usar mecanismos como DANE, onde está conexão técnica entre certificados e DNSSEC, e eu estou falando agora em nome pessoal, porque ainda não se discutiu isto em SSAC. Existe a possibilidade de que o proprietário de um domínio dentro do seu pais, obtenha uma CA, da sua cidade local, ou depois tenha uma rasto, pegada uma marca e tenha essa tecnologia no DANE se vincula ao DNSSEC e depois diga para aos outros que se conectam na internet que precisa de web que está procurando no nome do domínio, e isso é onde está o DNSSEC e DNS, esse cliente é proprietário desse website, vai encontrar a maneira de estar no DNS e valida-lo com a ajuda de DNS-CC. Essa marca está armazenada num correspondente, depósito ou repositório. E vemos que em alguns países, não só em desenvolvimento, mas já desenvolvidos, como a Suécia, hoje tem que acabar numa dessas

listas onde, alguns desses sistemas operacionais que são confiáveis, e é difícil para o CA porque o Ca querem se concentrar em enviar certificados de uma operação segura e sólida, e talvez esse é o lugar, o ponto, em que tem que se concentrar e não em estar em todos esses buscadores e listas de CA confiáveis. Então sim vejo uma conexão aí onde pode ser muito útil para inovação dentro de um âmbito seguro de CAs.

HEATHER: Muito obrigado pela resposta. Uma outra pergunta, ou algum cometário por parte do GAC, sobre este tema? Irão.

IRÃO: Obrigado Senhora Presidente. Muito obrigado pela apresentação e pelas respostas tão claras. Tenho uma pergunta muito simples. Como poderiam garantir que o domínio funcione, dentro dos termos e condições estabelecidas nos certificados? No sentido de que talvez seja alguma possibilidade de que não haja o cumprimento com esses termos e condições. Se for assim se a resposta for afirmativa como se vai monitorizar essa situação? Como é possível conseguir que simplesmente os termos e condições se sigam da maneira adequada?

PATRIK FALTSTROM: Eu apenas posso responder da perspectiva de DNS. Como disse, há acordos dentro do fórum de buscadores de CA e de melhoras praticas para as autoridades de CA e também para os CAs. Eu não sei o que é que estão utilizando como politicas e como auditoria, dentro desse fórum, teria que falar com eles. Em relação ao DNS os certificados em si

mesmos incluem os nomes de domínio que abrangem, o que cobrem, os certificados hoje. Esse nome de domínio no certificado pode incluir qualquer nome de domínio. Isso significa que o vínculo do anterior certificado e o proprietário do certificado e o nome de domínio é uma validação da autoridade. Do que autoridade de certificação está fazendo? Simplesmente estamos esperando isso, que as autoridades de certificação estão seguindo essa atividade. Esta nova tecnologia DANE, podemos utiliza-la exatamente para isto, porque permite que o proprietário de um certificado coloque uma marca, uma *checksum*, do certificado no DANE, sobre o nome de domínio especifico e não faça assinatura no DNSSEC. Então se eu não tivesse feito, como o proprietário de certificado, e vocês estivessem conectado ao meu web, primeiro teriam que utilizar o nome de domínio e validariam isto, e depois teriam que ver, no registo de DNS, para procurar a marca do certificado, que eu coloquei dentro do DNS. Verificariam essa assinatura de DNSSEC para estar certo de que essa marca seja certa. Agora conhecem o nome de domínio e sabem qual é o certificado, Depois procurariam o certificado e aqui vem a chave. Se verifica o nome do domínio dentro do certificado, e verificam que esse nome de domínio seja o mesmo que estavam olhando, estavam procurando e validando quando derem esse SEC. E se há essas duas coincidências vão saber que o certificado realmente foi emitido para esse nome de domínio o qual vocês estão tentando conectar com a ajuda do DNSSEC. Isso significa que com a ajuda de DNSSEC têm uma capacidade adicional como usuário final de validar que a autoridade de certificação estava a fazer o que devia fazer. E è por isso que é tão importante. Porque hoje uma autoridade de certificação pode emitir um nome de domínio para qualquer nome de domínio que ali estiver. É claro que há um

mecanismo de controlo e auditoria, mas nossos engenheiros adoram tomar medidas adicionais e super técnicas para isto.

HEATHER: Outro comentário do Irão?

IRÃO: Sim. Não é o mesmo que é o que se deve fazer ou o que se está fazendo?

PATRIK FALTSTROM: Hoje quando derem DNSSEC se uma resposta de DNSSEC não é validade, como cliente não vai receber essa resposta do seu computador. Hoje quando usam um buscador provavelmente têm uma tela a dizer "isto é inseguro, quer continuar? Sim, Não", todo o mundo faz SIM, clica em SIM. Nas novas tecnologias vocês não vão ter essa opção, então o utilizador final vai estar protegido. Mas em alguns casos vão receber o mesmo tipo de informação para o usuário final. Para que a aplicação possa informar, ao usuário final, que está digitando, que está entrando, numa comunicação que não é segura. Mas, é claro, como todos sabemos, preferimos comunicar-nos nesse jeito. Porque a comunicação em si própria é importante sempre quando saibamos que possa ser insegura.

HEATHER: Obrigado por essa pergunta e por essa resposta Patrick. Eu não sei se há algum comentário adicional, dos membros do GAC? Temos os relatórios disponíveis. Aqui se trabalhou sobre os certificados dos

nomes internos e também sobre a colisão de nomes. Então acho que é uma coisa muito útil para que o GAC possa continuar com a sua leitura. Se houver dúvidas adicionais certamente esse SSAC vai responder a qualquer consulta.

PATRIK FALTSTROM: Igual que em outras reuniões quero aproveitar para informar-lhes que temos quase 20 membros desse SSAC dos 39 do grupo, aqui em Durban. E todos eles estão mais do que dispostos a ajudá-los. Então não precisam de me procurar a mim pessoalmente. Há muitos especialistas na matéria que conhecem todos os pormenores da matéria, melhor do que eu. Se precisarem de um esclarecimento não duvidem em procura-los. Porque é isso para o qual temos que aproveitar estas reuniões. Para retomar as comunicações, relatórios, sentar com os membros da SSAC, e fazer as perguntas necessárias para entender um pouco mais todo o tema. È uma boa ideia, talvez os membros aqui presentes de SSAC, possam ficar em pé. Para poderem ser identificados. Esse aspeto temos.

HEADER: Bom é número bastante importante de pessoas. Muito obrigado por todas as informações. Vejo uma pergunta da Austrália.

AUSTRÁLIA: Obrigado Senhora Presidente. Obrigado Patrick. Foi uma discussão extremamente interessante. Já que á um par de minutos, e ainda não se falou sobre o tema, que é um relatório sobre os domínios sem ponto. E eu queria saber se pode fazer algum comentário a respeito. Eu li a posição da SSAC, que parece estar muito clara a partir desse relatório. È

uma recomendação muito rigorosa sobre, contra o uso, mas gostaria saber se continuam trabalhando sobre essa temática, então interessa-me saber se pode dar uma ideia da situação em que se encontra com os nomes sem ponto.

PATRIK FALTSTROM: Obrigado pela pergunta. Em primeiro lugar o guia do solicitante diz que o domínio sem ponto, que é como chamamos em SSAC, é uma coisa que não se permite, a não ser que o solicitante possa saber que esse uso é seguro. Nós analisamos esse tema em SSAC, fazemos uma recomendação ainda mais importante. De que por defeito a norma deve ser que haja uma delegação que o uso dos domínios sem ponto não seja autorizado. Durante o período de comentários publico que abriu o pessoal da ICANN, para o nosso relatório houve algumas respostas de fornecedores de provedores que diziam, até, que se os domínios sem ponto eram utilizados de facto para muitos utilizadores, usuários finais, haveria uma disrupção, do ambiente local. Então os mesmos fornecedores admitiam que era necessário não autorizar esse uso. E quando é utilizado um domínio sem ponto esse nome de domínio que utiliza o cliente nem sequer seria um *query* ou uma consulta de DNS. Porque as cadeias desse tipo não são procurados. Essa é a diferença. Depois disso o comité solicitou o pessoal da ICANN que emitisse um relatório sobre as implicações do tipo de vista económico ou financeiro de utilizar esses domínios. Mantivemos um diálogo sobre isto. O que aconteceu na Primavera foi que o pessoal da ICANN encomendou esse estudo sobre os domínios sem ponto que acho que estava finalizado, mas não á disposição do público. Mas em paralelo com esse estudo, que foi lançado, o comité de, o conselho de arquitetura fez um documento

sobre os padrões que estamos utilizando. A internet tem diferentes protocolos até o correio eletrónico, *email*, e deu também a sua recomendação contra o uso desses domínios sem ponto. Quer dizer que a recomendação é que não se utilize aqueles domínios sem ponto. Mas sabemos que o guia do solicitante, desde o início, recomendava a não utilizá-lo. Então todas as discussões surgiram por uma mudança requerida, mas o resultado é que o guia estava certo.

HEATHER: Obrigado. Argentina tem a palavra.

ARGENTINA: Obrigado Patrick pela apresentação e parabéns pelo trabalho feito. Tenho uma pergunta sobre grupo. Como são designados os membros desse SSAC? Eu vejo que na lista há apenas um membro da América Latina. O que poderíamos fazer nós, como representantes do GAC, para aumentar a diversidade no grupo, e se houver um desejo do grupo para ser mais diverso, vejo também que é mulheres, também poderíamos aumentar a quantidade de mulheres.

PATRIK FALTSTROM: Obrigado pela pergunta. Nós temos um grupo de trabalho que chama o comité de membros. Jim Calvin, é o presidente desse grupo e a lista nós recebemos nomeações, as pessoas podem nomear outras pessoas é feita uma entrevista a ele e o comité de membros tem uma lista das habilitações ou diferentes temas que são trabalhados. Através desses critérios que se identificam na entrevista. Por exemplo para este SSAC, é importante ter todas as habilitações requeridas, ou seja, poderão

analisar diferentes relatórios. Há pessoas que têm um conhecimento especializado em DNS, muito profundo. Não precisamos mais dessas pessoas, mas precisamos, como as ultimas designadas, pessoas que conheçam o mecanismo de aplicação da lei e que sejam mulheres também. È verdade que esse é um processo interno que nós seguimos. Nesse sentido e com relação á diversidade geográfica e de género, bem eu como presidente estou muito desiludido, pela situação em que estamos. Por isso sempre encorajamos outras pessoas para que se apresentem que se como candidatos.

HEATHER: Tenho pedidos de intervenção adicionais. Singapura a seguir.

SINGAPURA: Obrigado Senhora Presidente. Obrigado Patrick pelo trabalho realizado e pelo grupo. Tenho uma pergunta genérica. Sabemos que a industria á grupos de interesse que estão monitorando a segurança e estabilidade na internet. E há um grupo *anti-phishing*, dentro desse grupo. Já verificamos, nessa lista, os nomes desses sites. Queria saber qual é a relação entre esses sites e os grupos especializados da indústria? Como devemos abordar esse tema, se nós queremos alguma orientação, recorremos a esse SSAC ou um grupo como esse que é APWG? Não, não temos relação formal com nenhum dos grupos, temos membros desse SSAC também são membros da APWG, quer dizer que temos um grande volume de troca de informação entre esse APWG e PhishTank. e outros grupos similares.

HEATHER: A Rússia tem a palavra e depois Reino Unido.

RUSSIA: Obrigado senhor presidente. Patrick têm uma pergunta com relação á assessoria desse SSAC em relação aos domínios sem ponto. Deveria ser obrigatório essa recomendação ou é mais leve, porque não se pode aplicar a todos os TLDs. Porque já há alguns existentes ou há alguma limitação nas práticas?

PATRIK FALTSTROM: Como todos sabem, de modo que pontos, os registos de endereço no TLD estão no APEX da zona e a ultima vez, que eu, monitorei na internet continuava a funcionar. Tendo dito isso, em condições muito específicas, é possível utilizar um registo do endereço no APEX da zona, no APEX da zona, no índice da zona, e do ponto de vista técnico não se pode proibir isto da internet. Mas o risco é tão elevado que se deve desencorajar o uso.

RÚSSIA Tem mais a ver com as regras do jogo que é crítico. Do ponto de vista técnico eu sei que é um problema, mas isso tem a ver com as regras. Se a ICANN pode colocar requerimento para determinados registos e não para outros, isso poderia se problemático.

PATRIK FALTSTROM: Sim é verdade. Mas agora estamos passando mais para uma área que não tem tanto a ver com o nosso reconhecimento especializado, mas com acordos contratuais e com as partes contratuais. E nisso o SSAC

não tem gerência.

HEATHER. Obrigado. Reino Unido. Teima em fazer um comentário. Porque temos que fechar a sessão. Mas pediu a palavra? Pode ser breve por favor.

REINO UNIDO: Um aspeto que é do potencial de exploração criminal. Querem que o GAC dê assessoria no comité no sentido de dizer que parem?

PATRIK FALTSTROM: Parar o quê?

REINO UNIDO: A prática dos dominós sem ponto?

PATRIK FALTSTROM: Não seria ruim o apoio do GAC em termos de assessoria.

HEATHER: Uma resposta breve. Muito obrigado. Obrigado SSAC por ter assistido a esta reunião informativa que foi de grande valor para nós e quanto ao GAC temos 30 minutos de intervalo. Obrigado.