DIÁRIO DA ICANN 77- WASHINGTON, D.C. – DIA 1

ICANN 77 12 DE JUNHO DE 2023

Por Nivaldo Cleto*

Estamos em mais uma reunião da ICANN, desta vez a de número 77 na capital dos Estados Unidos, Washington, D.C., onde o grupo de usuários comerciais da Internet, Business Constituency (BC), vai avaliar as questões de governança na internet. Haverá também sessões técnicas sobre mitigação de abuso do Sistema de Nomes de Domínio (DNS[i]) e Extensões de Segurança DNS.

O BC é a voz dos usuários de internet comercial dentro da ICANN. O Grupo Constituinte representa os pontos de vista dos negócios da Internet e suas posições políticas são consistentes com o desenvolvimento de negócios por meio de uma Internet estável, segura e confiável, promovendo a confiança do consumidor.

No decorrer de toda esta semana, serão realizadas sessões da Organização de Apoio a Nomes com Códigos de Países (ccNSO[ii]), a comunidade de domínios de primeiro nível com código de país (ccTLD[iii]), com discussões sobre as tendências de registro para o período de 2019-2023 e sessão do Comitê Permanente de Abuso do Sistema de Nomes de Domínio (DNS) (DASC). Ele apresentará a segunda parte de suas conclusões da pesquisa de ccTLDs sobre abuso de DNS e lançará um repositório com informações úteis relacionadas ao abuso de DNS para a comunidade de ccTLDs. Confira aqui a sessão sobre abuso de DNS realizada no Fórum de Governança da Internet (IGF), em Addis Abeba, Etiópia, em dezembro de 2022.

Tech Day

Já nesta segunda (12) ocorreu o Tech Day, workshop aberto a todos os membros da comunidade da ICANN com interesse em tópicos técnicos, operacionais, de segurança e outros trabalhos relacionados ao DNS. Na ICANN 77, ele se concentrou nas extensões de segurança de DNS, prevenção e mitigação de abuso de DNS e outros tópicos.

SOBRE NIVALDO CLETO

Atua na área desde de 1978, foi presidente da Junta Comercial do Estado de São Paulo (Gestão 2001/2002)...

Saiba mais.

PESQUISAR

Search and hit enter...

RECENTES

Por fim, destaco o artigo abaixo, publicado no boletim informativo da Business Constituency, de Yusuph Kileo, membro do conselho da ICANN, sobre a importância de práticas segurança no meio digital para as pequenas empresas.

Como proteger sua pequena empresa com orçamento limitado

Por Yusuph Kileo, especialista em segurança cibernética e forense digital, BC-Rep (subcomitê financeiro), membro do Conselho da ICANN e do Grupo de Trabalho de Abuso de DNS do BC.

A noção de que você não é um alvo para invasores cibernéticos: que você, seus sistemas ou contas não têm nenhum valor é falsa. Se você usa a tecnologia de alguma forma, você tem valor para os cibercriminosos.

As ameaças cibernéticas vêm de várias formas, desde e-mails de phishing até ataques de ransomware. As pequenas empresas podem ser particularmente vulneráveis a ataques que exploram vulnerabilidades comuns, como software desatualizado ou senhas fracas.

De acordo com o estudo Cost of Cybercrime da Accenture, 43% dos ataques cibernéticos são direcionados a pequenas empresas, mas apenas 14% estão preparados para se defender. Quando as pequenas empresas se tornarem alvos de um ataque cibernético, eles podem acabar enfrentando consequências financeiras e operacionais, das quais alguns podem nunca se recuperar.

Infelizmente, a segurança cibernética pode não estar no topo da lista de prioridades da maioria das pequenas empresas. Mas deveria ser. A boa notícia é que existem etapas acessíveis você pode tomar para proteger sua empresa contra ataques cibernéticos.

IMPORTÂNCIA DA CIBERSEGURANÇA PARA PEQUENAS EMPRESAS

Avaliando seu risco

Identifique dados e ativos confidenciais: o primeiro passo para proteger sua empresa é identificar os ativos mais importantes para sua empresa. Isso inclui dados financeiros, informações de clientes ou propriedade intelectual.

Seus ativos também incluem o hardware sobre o qual sua empresa funciona. Se o hardware for tornado inoperável de um ataque cibernético, a incapacidade de realizar negócios pode ser igualmente devastadora.

Compreender o impacto potencial de uma violação de dados: Depois de identificar seus dados e ativos mais confidenciais, é importante entender o impacto potencial de uma violação de dados.

Considere como uma violação pode afetar seus clientes, suas operações comerciais e sua reputação.

Avaliando as medidas de segurança existentes: Avalie as medidas de segurança que você possui atualmente. Isso pode incluir tecnologia antimalware, firewalls ou programas de treinamento de funcionários. Procure lacunas em sua segurança e identifique áreas onde você pode melhorar.

Uma matriz de avaliação de risco pode ser usada para delinear a probabilidade e o impacto de um possível ataque cibernético. Isso permite que você priorize suas áreas mais vulneráveis.

Melhorando sua segurança cibernética

Implementação de protocolos básicos de segurança: Uma das etapas mais importantes para proteger sua pequena empresa é implementar protocolos básicos de segurança. Esses protocolos são projetados para proteger contra os tipos mais comuns de ataques cibernéticos e podem reduzir significativamente o risco de violação.

Gerenciamento de senhas: senhas fortes e exclusivas são uma parte crítica da boa higiene da segurança cibernética. Você deve incentivar seus funcionários a usar senhas complexas e difíceis de adivinhar. As ferramentas de gerenciamento de senhas são a melhor maneira de ajudar a controlar várias senhas exclusivas.

Monitoramento de rede: embora ferramentas como firewalls, sistemas de detecção de intrusão e software antimalware possam proteger sua rede contra ameaças cibernéticas, monitorar regularmente sua rede pode ajudar a identificar possíveis ameaças à segurança.

Um sistema de gerenciamento de log barato pode ajudar a identificar comportamentos suspeitos, como bloqueios de várias contas, bem como tentativas de login com falha e acesso não autorizado a arquivos.

Atualizações regulares de software: manter seu software atualizado é essencial para garantir que as vulnerabilidades sejam corrigidas e que seus sistemas estejam protegidos contra as ameaças de segurança mais recentes. Você deve atualizar regularmente seus sistemas operacionais, navegadores da Web e outros softwares para as versões mais recentes versões.

EDUCAR OS FUNCIONÁRIOS SOBRE AS MELHORES PRÁTICAS DE CIBERSEGURANÇA

Seus funcionários podem ser seu maior trunfo quando se trata de segurança cibernética, mas também podem ser uma responsabilidade se não forem treinados adequadamente. Educar seus funcionários sobre as melhores práticas de segurança cibernética é, portanto, crucial para proteger sua pequena empresa. Certas práticas das quais seus funcionários devem estar cientes incluem:

Evitando e-mails suspeitos: e-mails de phishing são uma tática comum usada por cibercriminosos para obter acesso a dados confidenciais. Instrua seus funcionários sobre como identificar e evitar e-mails suspeitos e considere implementar um software de filtragem de e-mail para reduzir o risco de ataques de phishing.

Não compartilhar senhas: Incentive seus funcionários a manter suas senhas privadas e nunca compartilhá-las com ninguém. Implemente a autenticação de dois fatores para adicionar um extra camada de segurança para o seu processo de login.

Protegendo dispositivos móveis: dispositivos móveis, como smartphones e tablets, podem ser um elo fraco em sua estratégia de segurança cibernética. Incentive seus funcionários a usar senhas fortes, habilitar atualizações automáticas e evitar o download de aplicativos suspeitos ou clicar em links em mensagens de texto.

Políticas e procedimentos de segurança cibernética: Estabeleça políticas e procedimentos claros que enfatizem a importância da segurança. Isso pode ajudar a garantir que todos estejam trabalhando em direção a um objetivo comum. Essas

cibernética. Nesse cenário, é importante responder de forma rápida e eficaz para minimizar os danos.

Na maioria dos casos, as técnicas forenses para descobrir o que causou o problema estão fora do alcance de muitas pequenas empresas.

A coisa mais importante para um pequeno empresário é voltar a funcionar o mais rápido possível.

É aqui que os backups de dados se tornam uma das ferramentas mais valiosas em um ambiente.

Outra maneira de se preparar e se recuperar de qualquer evento de segurança é contratar um provedor de serviços gerenciados confiável que possa aconselhá-lo e orientá-lo sobre a melhor segurança dentro do seu orçamento.

A segurança cibernética é um aspecto essencial da administração de uma pequena empresa no mundo digital de hoje. A prevalência de ameaças cibernéticas está aumentando, e o impacto de um ataque cibernético em uma pequena empresa pode ser devastador. Ao avaliar seu risco, implementar práticas recomendadas, criar uma cultura de segurança e fazer parceria com um consultor confiável, você pode proteger sua empresa dos perigos do crime cibernético.

Confira o artigo original : Como proteger sua pequena empresa

_____

(*) Nivaldo Cleto é empresário de contabilidade e de certificação digital, conselheiro do Comitê Gestor da Internet no Brasil CGI.br e membro da ICANN Business Constituency – BC

[i] DNS – (Domain Name System – Sistema de nome de domínio) converte nomes de domínio legíveis por humanos (por exemplo, www.amazon.com) em endereços IP legíveis por máquina (por exemplo, 192.0.2.44).

[ii] A Organização de Apoio a Nomes com Códigos de Países (ccNSO) é um órgão dentro da estrutura da ICANN criado para e por gerentes de ccTLDs. Desde sua criação em 2003, a ccNSO oferece um fórum para gerentes de domínios de primeiro nível (ccTLDs) de código de país se encontrarem e discutirem questões atuais de interesse dos ccTLDs de uma perspectiva global.

[iii] O domínio de topo de código de país ou domínio nacional de nível superior, é o domínio de topo na Internet geralmente usado ou reservado para um país ou um território dependente. Os identificadores de ccTLD são de duas letras.

LEIA TAMBÉM

Diário da ICANN 77- Washington, D.C. – Dia 3

16 de junho de 2023

ICANN 77 – Washington, D.C. – Dia 2

13 de junho de 2023

Diário da ICANN 77- Washington, D.C. – Dia 4

19 de junho de 2023

ICANN 77 – WASHINGTON, D.C. – DIA 2

ICANN 77 13 DE JUNHO DE 2023

(Na foto acima, Emily Taylor, CEO da Oxford Information Labs, membra da Chatham House e editora do Journal of Cyber Policy e Paulo Roque, presidente da Associação Brasileira das Empresas de Software – ABES)

Por Nivaldo Cleto*

Em nossa reunião regular da Business Constituency[i] (BC) dentro do evento presencial da ICANN em Washington D.C., tivemos algumas atualizações importantes de projetos apoiados por nosso grupo que buscam avançar nosso entendimento em relação ao DNS[ii] para continuar gerando políticas que criem um ambiente de Internet mais seguro para o meio empresarial.

Primeiramente, tivemos uma atualização da pesquisa intitulada "WhoisXML API research findings on DNS abuse", que explora tendências dos atores maliciosos dentro do espaço de nomes de domínios, no chamado Abuso do DNS. Um ponto importante que foi trazido é uma progressiva migração do abuso para o segundo nível dos domínios. Ou seja, ao invés de "abuso.net", estamos vendo cada vez mais "abuso.exemplo.net".

Isso não só é uma indicação de que devemos alterar os padrões que devemos observar quando buscamos atores maliciosos para prestar mais atenção para esse escopo aumentado, mas também sinaliza que os atores maliciosos estão percebendo a necessidade de inovar suas técnicas, o que é um possível indicador de que estamos conseguindo sucesso em combater as ações deles em certas dimensões.

SOBRE NIVALDO CLETO

Atua na área desde de 1978, foi presidente da Junta Comercial do Estado de São Paulo (Gestão 2001/2002)...

Saiba mais.

PESQUISAR

Search and hit enter...

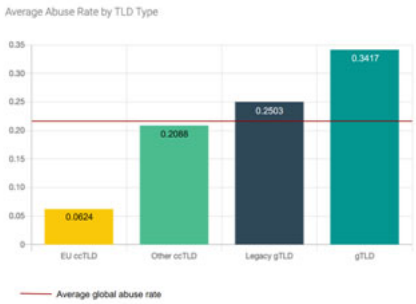
RECENTES

Também foi trazido à tona que os nomes de domínios mais antigos têm uma reputação por trás deles que pode ser aproveitada para evitar a checagem da detecção de domínios recém-registrados. Isso é algo que tem interessado os criminosos, que se aproveitam de domínios mais antigos que são abandonados por não serem renovados, por exemplo, e se aproveitam disso para mais facilmente se passar por um website legítimo.

Por fim, se confirmou que existe um crescimento de certos mercados de crime, e foi destacado o mercado da moda e marcas falsificadas como uma tendência. Foi trazido também que ocorrem pré-registro de domínios maliciosos visando coincidir com lançamentos de produtos altamente aguardados, como novos smartphones.

A segunda apresentação foi o "DNS Research Federation presentation on NIS2-related study", que abordou tendências de registros maliciosos dentro dos códigos de países (ccTLDs) da União Europeia, em vista de que, de modo geral, esses são vistos como casos de sucesso de contenção de registros maliciosos, buscando assim entender estratégias que poderiam ser utilizadas para outros provedores.

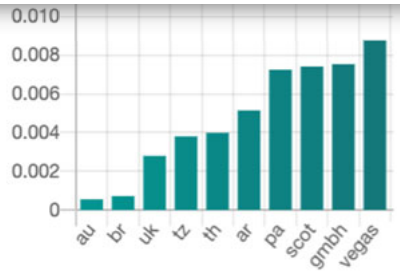
O estudo foi conduzido com base em dados coletados em 2022, e constatou que, de fato, a taxa de abuso observada nos ccTLDs da UE são os mais baixo em comparação com outros espaços estudados, mesmo quando é feito um controle baseado em custo dos domínios, algo que é frequentemente citado como algo que propulsiona a taxa de abuso em outros espaços.



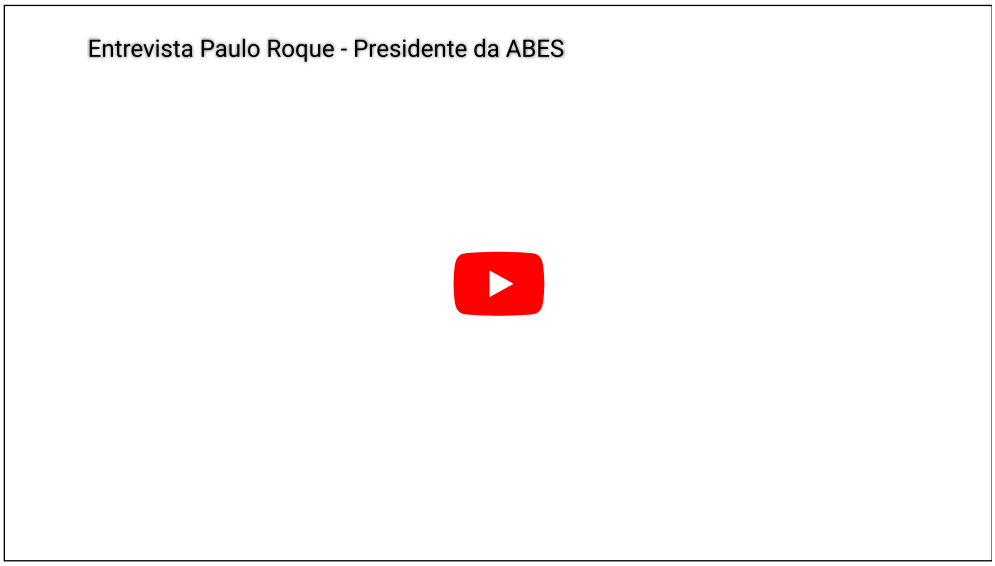
Quando foram buscados os motivos para essa melhor performance, não foi encontrado um fator determinante que pudesse ser entendido como uma prática única, mas sim uma série de lógicas que, quando combinadas, parecem gerar resultados positivos, dos quais podemos citar algumas questões.

Algo que parece ter influência é o fato de que esses países já operam em uma cultura de proteção de dados há diversos anos, algo que forçou muitas empresas digitais a se adaptarem e incorporarem práticas mais avançadas de segurança. Atrelado a isso, existe um envolvimento de atores locais com interesses atrelados aos ccTLDs[iii] que cobram ativamente por uma proteção dos nomes como uma marca. Foi observado também que a maioria dos registries responsáveis são organizações sem fins lucrativos.

Por fim, precisamos citar que a apresentação destacou a atuação do .BR como um ccTLD considerado altamente efetivo no combate de Abuso do DNS, com práticas sólidas que estão sendo reconhecidas internacionalmente.



Entrevista com Paulo Roque, presidente da Associação Brasileira das Empresas de Software (ABES)



(*) Nivaldo Cleto é empresário de contabilidade e de certificação digital, conselheiro do Comitê Gestor da Internet no Brasil CGI.br e membro da ICANN Business Constituency – BC

[i] O Grupo Constituinte de Usuários Comerciais de Negócios (também conhecido como Grupo Constituinte de Negócios, ou BC) representa os usuários comerciais da Internet. O Grupo Constituinte de Negócios é um dos Grupos Constituintes dentro do Grupo de Partes Interessadas Comerciais (CSG).

[ii] DNS – (Domain Name System – Sistema de nome de domínio) converte nomes de domínio legíveis por humanos (por exemplo, www.amazon.com) em endereços IP legíveis por máquina (por exemplo, 192.0.2.44).

[iii] O domínio de topo de código de país ou domínio nacional de nível superior, é o domínio de topo na Internet geralmente usado ou reservado para um país ou um território dependente. Os identificadores de ccTLD são de duas letras.

LEIA TAMBÉM

DIÁRIO DA ICANN 77- WASHINGTON, D.C. – DIA 3

ICANN 77 16 DE JUNHO DE 2023

Por Nivaldo Cleto*

Em nosso terceiro Diário da ICANN 77, discutiremos uma série de temas relevantes trazidos durante as discussões da comunidade com o comitê governamental (GAC)[i], que atua como aconselhador de políticas, mesmo que não de modo votante. Essas discussões são importantes para que os governos tenham ciência do que se passa dentro da ICANN e possam se planejar adequadamente. (Na foto acima, delegação brasileira na ICANN 77)

Um tema importante é a rodada subsequente de novos nomes de domínio genéricos. Esse conjunto de discussões terá como resultado o estabelecimento das regras e processos que permitirão que um novo processo de venda de sufixos (como o ".org") possa ser proposto e que diferentes partes interessadas do mundo possam fazer propostas que sejam apreciadas pela comunidade da ICANN.

Foi ressaltado que existe uma expectativa de que o GAC possa participar de modo igualitário do processo de tomada dessas decisões, em vista de ser um tema potencialmente sensível aos Estados. Isso está contido na versão atual do documento desenvolvido pelo Conselho de nomes genéricos[ii] (GNSO Council).

Um ponto que é contencioso é o de PICs (ou RVCs, sigla para Public Interest Committment), que são conjuntos de intenções que podem ser adotadas por registries que queiram exercitar algum tipo de governança voluntária em seus domínios. Para dar um exemplo fictício, em um domínio registrado debaixo do TLD ".futebol", poderia se prometer que não se permitiria nenhum website de apostas.

Os PICs foram amplamente utilizados na rodada de novos domínios de 2012, mas uma preocupação da comunidade é a pergunta de se esses compromissos são executáveis, pois é danoso que uma provisão dessas esteja em um contrato que não seja executável. O que se busca agora é progredir de uma questão teórica para a prática, garantindo que o setor de Compliance da ICANN possa aferir se um registry está em conformidade ou não.

SOBRE NIVALDO CLETO

Atua na área desde de 1978, foi presidente da Junta Comercial do Estado de São Paulo (Gestão 2001/2002)...

Saiba mais.

PESQUISAR

Search and hit enter...

RECENTES

Cartilha ensina como se proteger de códigos maliciosos na internet
FGTS Digital: empregadores poderão acessar a partir de agosto
A importância da contabilidade para a gestão das empresas
Receita Federal cruza informações financeiras
Diário da ICANN 77- Washington, D.C. – Dia 4
Diário da ICANN 77- Washington, D.C. – Dia 3

Reunião com os membros da LAC presentes na ICANN77

Além disso, existe uma complexidade relativa à própria ICANN, pois um PIC não pode contradizer algo que é explicito nas regras já existentes na organização. Isso causa uma cadeia de dependências complexa. A sugestão que o GAC fez de abordar a exigibilidade por meio de cláusula contratual só nos leva até certo ponto. Existem maneiras, por meio dos mecanismos de responsabilidade da ICANN, de questionar se algo é aplicável. Isso pode ser útil na resolução dessa questão.

A membra do Conselho Diretor, Avri Doria, acredita que os PICs podem ser executados dentro dos estatutos que temos atualmente, mesmo que outros diretores tenham opinião oposta. Faz parte do escopo da missão da ICANN permitir os PICs para que esses possam refletir questões de políticas públicas. Agora se faz necessário o trabalho da comunidade para desemaranhar as questões pendentes.

Papo Direto ICANN 77 – Entrevista com Andrea Beccalli representante da ICANN na Europa

(*) Nivaldo Cleto é empresário de contabilidade e de certificação digital, conselheiro do Comitê Gestor da Internet no Brasil CGI.br e membro da ICANN Business Constituency – BC

[i] O GAC constitui a voz dos governos e organizações intergovernamentais (IGOs) na estrutura multissetorial da ICANN. Criado de acordo com os Estatutos da ICANN, o GAC é um comitê consultivo da Diretoria da ICANN. A principal função do GAC é aconselhar a ICANN sobre questões de política pública e,

DIÁRIO DA ICANN 77- WASHINGTON, D.C. – DIA 4

ICANN 77 19 DE JUNHO DE 2023

Por Nivaldo Cleto*

Nesse quarto e último diário da ICANN 77 discutiremos o tema mais quente da reunião, que irá potencialmente afetar todos os nomes de domínios genéricos em existência (ou seja, aqueles que não são de países como o ".br"). Esse processo, conhecido como "*contract ammendments*", é uma negociação extraordinária que está envolvendo toda a comunidade ICANN, em busca de uma melhora dos padrões de cibersegurança do DNS[i].

Histórico

A ideia de atuar mais fortemente em cima do tema de combate ao Abuso do DNS data de 2019, quando os registries e registrars (Partes Contratadas) apresentaram o "DNS Abuse Framework", um documento voluntário que aumentava as obrigações daqueles que assinassem em relação a combater abuso técnico na Internet. Apesar de uma adesão alta, essa é uma indústria global com muitos atores e modelos de negócio, então diversos atores acabaram não assinando o documento.

Em 2022, o Conselho de nomes genéricos (*GNSO Council*) iniciou uma discussão sobre como preencher as expectativas da comunidade a respeito do tema, resultando em um grupo de trabalho liderado pelo Conselheiro originário do Brasil e parceiro da AR-TARC/NCCA, Mark Datysgeld. Depois de extensas discussões, o grupo decidiu por tentar uma maneira pouco usual de resolver o problema rapidamente: pedir diretamente para as Partes Contratadas que ponderassem as cláusulas de seus contratos relativas a abuso do DNS, destacando uma provisão em específico, a Seção 3.18.

Essa seção possuía requerimentos extremamente vagos sobre quais eram as obrigações das Partes Contratadas. Em consulta com o setor de Compliance da ICANN, o grupo descobriu que, de fato, muito pouco podia ser feito pela ICANN no caso de um ator particularmente malicioso abusar da infraestrutura do DNS, mesmo que o comportamento seja repetitivo e amplamente documentado.

Isso levou o grupo de trabalho a pedir, em carta pública, a negociação dos requerimentos da Seção 3.18. A decisão de aceitar ou não esse pedido estava totalmente nas mãos das Partes Contratadas, então foi recebido com grande entusiasmo por nós representantes dos interesses das pequenas e médias empresas que a sugestão tinha sido aceita, levando a um processo de negociação árdua entre o time legal da ICANN e as Partes Contratadas.

Resultados

Foi entendido pelas Partes Contratadas que o objetivo era levantar o piso do contrato, estabelecendo um padrão mínimo de obrigações relativas a abuso. Para isso, foi especificamente criada uma nova provisão, a Seção 3.18.2, que cria a obrigação da Parte Contratada "de tomar medidas de mitigação para interromper o abuso de DNS". Isso é também apoiado por uma série de

SOBRE NIVALDO CLETO

Atua na área desde de 1978, foi presidente da Junta Comercial do Estado de São Paulo (Gestão 2001/2002)...

Saiba mais.

PESQUISAR

Search and hit enter...

RECENTES

Cartilha ensina como se proteger de códigos maliciosos na internet
FGTS Digital: empregadores poderão acessar a partir de agosto
A importância da contabilidade para a gestão das empresas
Receita Federal cruza informações financeiras
Diário da ICANN 77- Washington, D.C. – Dia 4
Diário da ICANN 77- Washington, D.C. – Dia 3

Encontro com a comunidade da América Latina e Caribe durante a ICANN 77

Fica também reforçada a definição de Abuso do DNS como sendo relativa aos casos de: malware, botnets, *phishing*, *pharming*, e spam quando é um mecanismo de entrega para outras formas de abuso listadas. Isso significa que questões diretamente relacionadas a assuntos como propriedade intelectual continuam a não ser diretamente contemplados, dependendo de ações diretas com os tribunais e agências de polícia.

No entanto, os empresários passam a ter uma nova ferramenta em vista de que muito do abuso que é praticado contra o setor comercial vem na forma de golpes de imitação de um outro website (*phishing*), direcionado aos clientes de uma dada marca. Passa a ser consistente a possibilidade de retirar do ar esse tipo de material, pois seria provisionado de maneira global para todos os nomes genéricos.

No entanto, é muito importante ressaltar que essa negociação depende agora de uma etapa crítica: a votação final que será feita em alguns meses pelas Partes Contratadas. É necessário que 90% deles esteja de acordo com as mudanças para que elas sejam adotadas de maneira uniforme. Existe uma expectativa positiva em relação a essa votação, mas sempre existe a possibilidade de ela falhar.

Dessa forma, **é necessária ação da comunidade empresarial**. Todos os empresários devem entrar em contato com as empresas responsáveis pelo registro de seus domínios que não sejam códigos de países (ficando assim excluídos os domínios ".br", mas incluindo aqueles como ".com", ."net", ".org", ".info" e outros) e notifica-los sobre a necessidade de votar na aprovação das mudanças contratuais relativas a Abuso no DNS na ICANN.

Se formos bem-sucedidos, teremos trazido mais uma vitória para a comunidade mundial de pequenos e médios empresários. Teremos mais atualizações em alguns meses, nos Diários da ICANN 78, que se dará na Alemanha.

(*) Nivaldo Cleto é empresário de contabilidade e de certificação digital, conselheiro do Comitê Gestor da Internet no Brasil CGI.br e membro da ICANN Business Constituency – BC

[i] DNS – (Domain Name System – Sistema de nome de domínio) converte nomes de domínio legíveis por humanos (por exemplo, www.amazon.com) em endereços IP legíveis por máquina (por exemplo, 192.0.2.44).

LEIA TAMBÉM