ICANN82 | Semana de preparação – Atualização de conformidade contratual
Segunda-feira, 24 de fevereiro de 2025 – 12h30 a 13h30 PST

JONATHAN DENISON Olá e bem-vindos à atualização do Programa de Conformidade Contratual antes do webinar do ICANN82. Meu nome é Jonathan Denison e sou gerente de participação desta sessão. Lembrem-se de que esta sessão está sendo gravada e é regida pelo padrão de comportamento esperado da ICANN e pela política antiassédio da comunidade da ICANN.

Durante a sessão, os comentários ou perguntas serão lidos em voz alta apenas se forem enviados no espaço de perguntas e respostas. A sessão será interpretada em inglês, francês e espanhol. Todas as sessões da semana de preparação terão transcrições em árabe, chinês, inglês, francês, português, russo e espanhol. Se alguém quiser falar durante a sessão, basta levantar a mão no Zoom. Quando dissermos seu nome, ative o microfone para falar. Diga seu nome e o idioma em que vai falar caso não seja em inglês. Fale devagar.

Nesta sessão, falaremos sobre a aplicação dos requisitos de mitigação de abusos do DNS, a aplicação dos requisitos do RDAP, a auditoria de conformidade contratual e o apoio às iniciativas de políticas e grupos de trabalho. Confiram instruções sobre como enviar perguntas e/ou comentários na caixa de bate-papo. Vou

publicar tudo isso logo após a sessão. Agora, passo a palavra para Jamie Hedlund, vice-presidente sênior de conformidade contratual e interação com o governo dos EUA. Obrigado.

JAMIE HEDLUND

Obrigado, JD. Olá a todos e obrigado por participar da atualização sobre o programa de conformidade. Como JD mencionou, meu nome é Jamie Hedlund, sou líder de conformidade contratual da organização da ICANN.

A comunidade da ICANN desenvolve políticas consensuais relacionadas à segurança, estabilidade e flexibilidade do DNS (Sistema de Nomes de Domínio) da Internet. Após a adoção pela Diretoria, a organização da ICANN incorpora essas políticas aos nossos acordos contratuais com registros e registradores. A principal função da Conformidade da ICANN é garantir que os registros e registradores implementem essas políticas desenvolvidas pela comunidade e cumpram com todas as obrigações contratuais para preservar e aprimorar a segurança, estabilidade e flexibilidade do DNS.

Colocamos essas obrigações em vigor resolvendo reclamações externas, conduzindo auditorias regulares das partes contratadas e realizando iniciativas proativas de aplicação. Temos um compromisso com a transparência e com a publicação regular de métricas e dados sobre atividades relacionadas a reclamações e ações de aplicação. Apoiamos iniciativas de políticas e negociações de contratos, fazendo comentários sobre a clareza e a

viabilidade das obrigações propostas, além da aplicação do processamento de reclamações e dados sobre aplicação para embasar discussões sobre as obrigações existentes.

Por último, participamos de sessões de treinamento e divulgação no mundo todo para aumentar a conscientização em relação a obrigações contratuais entre a comunidade. Agora, para fazer um resumo das atividades de mitigação de abusos do DNS, passo a palavra ao meu colega Romulo Chacin. Romulo?

ROMULO CHACIN Obrigado, Jamie. Posso falar? Perfeito, obrigado. Olá a todos. Meu nome é Romulo Chacin e vou fazer uma apresentação sobre a aplicação dos requisitos relacionados ao abuso do DNS. Então, começando, em 5 de abril de 2024, novos requisitos relacionados à mitigação de abusos do DNS entraram em vigor no Contrato de Credenciamento de Registradores e no Contrato Básico de Registro. Nesse dia, a Conformidade Contratual da ICANN começou a aplicar os requisitos e fazer denúncias.

De forma geral, agora temos uma definição de abuso do DNS. Para a finalidade do Contrato de Credenciamento de Registradores e do Contrato Básico de Registro, isso significa malware, botnets, phishing, farming e spam, quando o spam é usado para entregar um ou mais dos outros quatro tipos de abuso do DNS. Além disso, agora as partes contratadas precisam tomar medidas de mitigação

com a meta de impedir ou de alguma forma impossibilitar o uso de nomes de domínio para abusos no DNS.

Há um esclarecimento de que o e-mail ou formulário da web dedicado a abusos das partes contratadas deve estar facilmente acessível em seus sites, e há um requisito para que as partes contratadas confirmem que sua denúncia de abuso foi recebida. A organização da ICANN produziu um informe com orientações e informações sobre como aplicamos esses requisitos. Esse informe está disponível no site da organização da ICANN e também tem um link na parte inferior deste slide para vocês consultarem. Agora, com esses requisitos em mente, podemos ir para esse slide. Obrigado. Vou passar a palavra para Leticia Castillo.

LETICA CASTILLO

Obrigada, Romulo. Olá a todos. Sou Leticia Castillo. Romulo deu uma explicação geral dos requisitos de mitigação de abusos do DNS que começamos a aplicar no ano passado. Na nossa última atualização sobre o programa, fornecemos algumas métricas relacionadas aos primeiros seis meses de aplicação desses requisitos. E hoje, vou compartilhar algumas atualizações sobre as iniciativas em que estamos trabalhando e números atualizados, incluindo dados de 5 de abril de 2024 até 5 de dezembro de 2024.

Como vocês podem ver neste slide, durante esse período, lançamos 249 investigações com registradores e registros em relação aos requisitos de mitigação de abusos do DNS. A maioria dos casos envolviam phishing, seja sozinho seja junto com outros

tipos de abuso ou abuso do DNS. Conforme os relatórios, os nomes de domínio foram usados para se passar por instituições governamentais, lojas online, entidades financeiras e outros. Duas das investigações levaram a notificações formais de violações, uma para um registro e outra para um registrador.

Em 5 de fevereiro, emitimos outra notificação formal de violação a outro registrador, relacionada a um caso de phishing com um nome de domínio direcionado a uma empresa que oferece serviços financeiros no mundo todo. Durante esse período, também resolvemos mais de 200 investigações de abuso do DNS por meio de resolução informal. Isso sem necessidade de notificação formal de violação, levando à suspensão de mais de 2.900 nomes de domínio abusivos e à desativação de mais de 365 sites de phishing.

A etapa de resolução informal é onde a maior parte das nossas investigações são resolvidas em praticamente todos os tipos de denúncias. Isso porque a parte contratada comprova a conformidade ou resolve uma não conformidade antes que a denúncia chegue a uma etapa formal. Quero destacar que, embora as notificações de violação sejam importantes, elas não são a única indicação de que a aplicação está acontecendo. A aplicação, remediação e inação acontecem mesmo que não sejam refletidas em uma notificação pública de violação, como indicam os mais de 200 casos resolvidos.

Também é importante ressaltar que a Conformidade da ICANN tem visibilidade do nome de domínio e dos casos que estão sujeitos às

nossas denúncias, não de todo o ecossistema de DNS e de todas as medidas que os registradores e registros tomam para combater o abuso do DNS e cumprir com suas obrigações contratuais sem que a Conformidade da ICANN os contate.

Em junho de 2024, começamos a publicar relatórios relacionados à aplicação dos novos requisitos de mitigação de abusos do DNS. Esses relatórios são divididos por tipo de abuso do DNS. Eles começam com dados de abril de 2024 e são atualizados todos os meses. E temos complementado essas métricas mensais com blogs e relatórios que incluem mais contexto e exemplos semelhantes ao que publicamos em 8 de novembro para os seis meses de aplicação. E também divulgaremos um relatório após concluir a auditoria de registro em andamento, que inclui requisitos de mitigação de abuso do DNS.

Próximo slide, por favor. Obrigado. Como mencionei antes, as notificações de violação são emitidas quando a etapa de resolução informal do nosso processo termina sem resolução. Essas notificações são públicas. Elas relacionam as violações identificadas e que medidas precisam ser tomadas para resolvê-las. Em relação aos requisitos de mitigação de abusos do DNS, especificamente, emitimos três notificações formais de violações até agora. Duas para registradores, uma para um operador de registro. De acordo com os contratos, os registradores tiveram inicialmente 21 dias para resolver o problema, enquanto o registro teve 30 dias para entrar em conformidade. Três notificações de violação estão abertas. Os notificados receberam extensões nos

prazos enquanto contratam as partes para continuar trabalhando ativamente na correção e na conformidade.

Próximo slide, por favor. Não é algo incomum estender os prazos das notificações de violação quando certos requisitos são atendidos. E isso inclui que o registrador ou registro tenha tomado medidas de mitigação em todos os nomes de domínio abusivos denunciados, não apenas no caso inicialmente identificado, mas, em alguns casos, em nomes de domínio adicionais descobertos ao longo da investigação específica. Então, para deixar claro, nenhuma extensão será concedida se os nomes de domínio abusivos continuarem ativos e prolongando a exposição de possíveis vítimas ao abuso do DNS.

Por exemplo, uma das notificações de violação foi emitida para um caso envolvendo mais de 90 domínios. Hoje em dia, mais de 5 mil domínios já foram mitigados depois da notificação de violação. Ainda não incluímos o número em nossos relatórios porque a questão está aberta e estamos identificando domínios mitigados resultantes de casos resolvidos, mas incluiremos esses números atualizados em nossos futuros relatórios. Continuamos colaborando com a parte denunciante que foi muito responsiva e forneceu informações adicionais. Continuamos investigando e trabalhando com a parte contratada para garantir que medidas de mitigação sejam tomadas em um processo implementado, mas essa questão continua em aberto.

Também concedemos extensões apenas se a parte contratada tiver apresentado um plano de remediação detalhado, com um cronograma razoável levando em conta as alterações necessárias e demonstrando que as diferentes etapas do plano estão sendo implementadas. Por exemplo, se a etapa um do plano deve ser concluída até 4 de dezembro, em 5 de dezembro, exigiremos a confirmação de que isso foi feito, incluindo os testes necessários. Também continuaremos considerando extensões adicionais para as etapas restantes do plano conforme necessário e apropriado.

Além disso, é importante lembrar que essa é uma questão complexa. A ICANN também exige tempo para analisar e, quando aplicável, testar diferentes etapas do plano e comunicar o feedback, solicitações de informações e ações. Então, isso também é levado em conta ao fornecer extensões. Incluiremos mais detalhes sobre o status da notificação de violação e de futuras notificações em nossos próximos relatórios.

Próximo slide, por favor. Então, qual é o próximo passo? Vamos continuar aplicando os requisitos que temos desde o dia em que entraram em vigor e que monitoramos. Não apenas por meio do nosso painel mensal, também pretendemos divulgar um relatório anual de aplicação, como fizemos com um relatório semestral, incorporando também alguns dos comentários que recebemos sobre esse relatório.

Lançamos uma auditoria de registro em outubro, que ainda está em andamento. Joe vai falar mais sobre isso mais adiante. Essa

auditoria incluiu requisitos de abuso do DNS, e publicaremos o relatório quando for concluído. Também estamos preparando uma auditoria de registradores que também incorporará requisitos de mitigação de abusos do DNS.

No relatório semestral, mencionamos como estamos trabalhando em iniciativas relacionadas à facilitação do envio de denúncias práticas para nós, incluindo a produção de diretrizes e outros materiais para denunciantes. Estamos trabalhando nisso. Ainda não temos uma data de publicação, mas os documentos estão redigidos, e toda a equipe de processadores revisou os dados que coletamos ao longo dos meses e compartilhou nossa própria experiência. Acreditamos que fornecer esse tipo de orientação adicional aos denunciantes será benéfico, então fiquem ligados.

E, por fim, considerando a experiência que adquirimos e continuamos a adquirir ao longo do mês na aplicação desses novos requisitos, estamos trabalhando para elaborar esforços de aplicação mais proativos. Mais uma vez, ainda não temos uma data de lançamento. Está em fase de design, mas algo importante a ter em mente é que nunca nos limitamos aos detalhes das informações e às denúncias que recebemos. Sempre conduzimos uma análise abrangente de cada caso. Observamos e investigamos padrões.

Também temos o monitoramento proativo em forma de auditoria e agora estamos elaborando uma iniciativa estruturada para iniciar proativamente ações de aplicação para abuso de DNS que,

combinadas com nossa aplicação diária por meio do processamento de denúncias e do programa de auditoria, continuarão a demonstrar nosso compromisso contínuo em manter os novos requisitos. Então, temos muitas novidades pela frente. Fiquem ligados. Agora, vou passar a palavra para Amanda e, no final, vou responder às perguntas de vocês. Obrigada.

AMANDA ROSE Obrigada, Leticia. Podemos prosseguir. O próximo tema é a aplicação dos requisitos de RDAP, que vou apresentar. O primeiro slide fala do estado atual dos requisitos e em que etapa estamos em termos de serviços de diretório de dados de registro. Desde fevereiro de 2024, tanto os registradores quanto os operadores de registro devem estar em conformidade com todos os requisitos do RDAP, aqueles que os incorporaram em seus acordos, o que inclui todos os registradores e a maioria dos operadores de registro.

Esses requisitos incluem a importação ou implementação do perfil de resposta, além do guia de implementação técnica. Esses requisitos expandem basicamente a necessidade de ter um serviço RDAP geral, que é o que estávamos aplicando antes da data de aplicação em fevereiro. Então, isso basicamente ensina como implementá-lo exatamente do ponto de vista técnico, mas também quais informações devem ser retornadas em uma resposta de consulta ao RDAP.

Então, agora, há duas versões do perfil de resposta e do guia de implementação técnica. Tem a de fevereiro de 2019 e a de

fevereiro de 2024. A versão de fevereiro de 2024 é a nova, para se alinhar às mudanças nos requisitos relacionados à política de dados de registro. Então, até 21 de agosto de 2025, este ano, a versão de fevereiro de 2024 deve ser implementada e, novamente, ela está alinhada com esses requisitos, então a data efetiva da política de dados de registro é essa mesma data. Até então, é possível implementar a versão de 2019 ou a de 2024.

Os requisitos adicionais incluem requisitos de nível de serviço. Então, estão no acordo de registro de base e no RAA. Também começamos o monitoramento automatizado desses requisitos, que estão sendo incorporados em nossos processos de conformidade. Os registradores têm o requisito de fornecer um nome registrado à ICANN. Ele será usado em nossos testes e como fazemos pesquisas no serviço RDAP. Então, uma vez que é fornecido, é usado para monitorar e testar a conformidade com o guia de implementação técnica e o perfil. No caso de quem não fornecer esse nome, usaremos um nome de domínio aleatório, então obviamente é bom ter esse caso de teste.

Então, em termos de onde estamos em relação ao RDAP ou aos serviços de diretório, a data de desativação do WHOIS já passou. Foi em 28 de janeiro deste ano. Nesse momento, a maioria das partes contratadas, registradores e operadores de registro, não precisam mais oferecer serviços de WHOIS. Muitas ainda oferecem, e essa é uma opção nos acordos, continuar oferecendo o WHOIS. Se fizerem isso, eles terão que continuar cumprindo certos requisitos, como os requisitos da política de dados de registro ou a

especificação temporária neste momento, que é a política provisória. Mas eles também podem fazer uma exibição truncada e, nesse caso, precisam incluir uma mensagem encaminhando o autor da consulta ao serviço RDAP para que ele saiba que, naquele momento, o WHOIS pode não fornecer todas as informações, então precisamos ir para uma nova fonte de dados.

Podemos passar para o próximo slide. Em termos de aplicação, aplicamos o requisito de ter um serviço, como mencionei antes. Isso começou em outubro de 2019, e acredito que temos cerca de 12 partes contratadas, registradores que não forneceram um serviço RDAP básico, ou sua URL, que precisa atender a um teste mínimo dos serviços da IANA. Então, isso não inclui o perfil e o guia de implementação técnica. E, como disse no slide anterior, não iniciamos a aplicação dessas normas até que as emendas fossem incorporadas aos acordos, incluindo esses requisitos.

Então, intensificamos a aplicação desde que as emendas entraram em vigor e o período de aceleração da implementação do RDAP terminou. Desde então, emitimos 15 notificações formais de violação que incluíram requisitos do RDAP para corrigir a não conformidade com o RDAP nas notificações de violação. Uma dessas notificações foi enviada porque o serviço de RDAP não foi prestado, e isso levou à rescisão do contrato de credenciamento do registro.

Com respeito à maioria dos outros casos que estão em processamento ou encerrados, continuamos monitorando os

serviços de RDAP. E, devido à natureza técnica desses tipos de casos, aqueles que estão sendo corrigidos ou entrando em conformidade nos fornecem atualizações regulares semelhantes ao que Leticia descreveu com relação às alterações de abuso de DNS, exigindo que eles cumpram certos marcos e expliquem qual processo têm em vigor e o que estão fazendo para garantir que seu RDAP esteja em conformidade com esses requisitos.

Podemos passar para o próximo slide. Esses são alguns dos problemas de não conformidade comuns que enfrentamos. Os primeiros são os requisitos do guia de implementação técnica, e é melhor que o pessoal técnico fale sobre eles, mas é o que vemos. Há um cabeçalho de tipo de conteúdo que precisa ser definido especificamente para o código "application/RDAP+JSON". Então, quando eles não são definidos, nosso sinalizador de conformidade é exibido, e esses serviços de RDAP podem falhar mesmo quando estiverem funcionando em lookup.ican.org, por exemplo. Outros clientes web podem não ser capazes de analisar os dados, retornando um erro.

Se alguém esteve na apresentação do RDAP mais cedo, acho que Andy Newton disse que existem aproximadamente de 30 a 40 clientes web variados além de lookup.icann. Então, é importante que eles sejam compatíveis, e isso faz parte dos requisitos de tipo de conteúdo.

O outro problema comum que encontramos é que o serviço de RDAP é fornecido apenas em IPv4. É obrigatório que seja fornecido

em IPv4 e IPv6. Outro problema que costumamos encontrar é que isso é fornecido por HTTP, e precisa ser apenas HTTPS, então isso é sinalizado como problema de segurança. O último e menos comum dos problemas que encontramos é quando os serviços de RDAP não retornam um status 200 HTTP. Basicamente, se o domínio for patrocinado pelo registrador, ele precisa retornar um status 200 OK, e se não for patrocinado, precisa retornar um status 404 não encontrado.

Em termos de perfil de resposta, vou dizer ao contrário, mas uma das principais coisas que vejo cada vez mais agora é que os dados de registro exigidos pelos contratos estão faltando na resposta do RDAP. Os contatos do registrante e, às vezes, os contatos administrativos e técnicos, ou até mesmo o registrador, podem estar ausentes, ou os contatos de abuso. Estão totalmente ausentes, e isso é um problema com o próprio perfil de resposta. Outro problema é que os status do EPP podem não ser mapeados corretamente, porque os antigos status do WHOIS foram alterados no RDAP para os status obrigatórios do RDAP.

E o último problema, que é sério. O perfil descreve exatamente como as notificações devem ser no RDAP. Elas também eram exigidas com o WHOIS, mas itens como a referência aos códigos de status e o que eles significam, se não forem correspondidos ou formatados corretamente, serão sinalizados como fora de conformidade, e esse problema também deve ser resolvido. Existem muitos outros. Analisando o guia de implementação técnica e os perfis de respostas, vocês verão muitos requisitos.

Então, temos muito trabalho pela frente. Às vezes, são casos fáceis, abertos e fechados rapidamente. Mas, muitas vezes, não é assim. Então, este é apenas um resumo rápido de alguns problemas comuns que encontramos.

E o último slide tem alguns dos nossos recursos. A ICANN desenvolveu uma ferramenta de conformidade com o RDAP. Ela está disponível online e também no GitHub, e essas informações também estão disponíveis na apresentação do RDAP. Então, essa ferramenta pode ser executada localmente em um disco ou sistema, e também na web. Recomendamos que todas as partes contratadas testem.

Uma observação é que, no momento, ela é compatível apenas com o perfil do RDAP de 2019 e com o guia de implementação técnica. Estamos trabalhando na atualização para a compatibilidade com as versões de fevereiro de 2024. Mas também vale lembrar que ela sinaliza problemas nas duas versões.

Então, o guia de implementação técnica é amplamente baseado nos RFCs atuais e não muda entre as versões. Então, todas essas sinalizações ajudam ou ainda funcionam para quem implementou ou caso a parte contratada tenha implementado as versões de fevereiro. Há muitas semelhanças. Alguns pequenos itens precisam ser atualizados, mas é bom usar a ferramenta de qualquer forma.

Tem outro link para a wiki da ferramenta de conformidade do RDAP. Nossos colegas do serviço técnico trabalharam para

fornecer recursos que ajudam a explicar muitas das informações nas ferramentas de conformidade. Isso é muito útil na implementação, além de diagnostica problemas que apareceram.

E o último é o guia do RDAP. Esse é o recurso terceirizado de Andy Newton, mas é bastante informativo em relação aos requisitos do RDAP para qualquer pessoa curiosa. E ele gentilmente nos deixou compartilhar o recurso, o que acho útil também do ponto de vista de conformidade para pessoas que talvez não tenham tanto conhecimento técnico para ajudar a entender o que é necessário. Com isso, acho que podemos passar para a auditoria. Joe Restuccia.

JOE RESTUCCIA Obrigado, Amanda. Olá a todos. Sou Joe Restuccia. Sou membro da equipe de auditoria de conformidade e vou destacar a auditoria atual e em andamento. A auditoria foi iniciada no final de outubro do ano passado, e é uma auditoria completa, o que significa que vamos testar todas as obrigações que normalmente testamos e que fazem parte do acordo de registro e das políticas da ICANN.

Mas algo importante a observar é que, além disso, também vamos testar os novos requisitos de abuso do DNS. Os testes relacionados a esses requisitos se concentram em verificar que os registros entendam suas obrigações e que tenham os processos necessários em vigor para resolver os abusos do DNS. O estágio atual da auditoria é que todos os auditados responderam à nossa solicitação de informações, e a equipe de auditoria está revisando

todas essas respostas, toda a documentação que recebemos, e estamos fazendo perguntas de acompanhamento e buscando informações ou documentos adicionais conforme necessário.

Após a auditoria, vamos publicar um relatório final. Será público, então vocês poderão vê-lo. É um relatório que sempre publicamos ao final de cada auditoria. Ele incluirá muitas coisas, entre elas um resumo geral da auditoria, além de informações adicionais sobre as nossas conclusões. Com isso, passo a palavra a Jonathan Dennison.

JONATHAN DENISON Ok, sou eu. Voltei com lembretes regulares sobre algumas das outras atividades em que a conformidade está envolvida, além de abordar casos de conformidade. Alguns de vocês já sabem, é claro, que somos colaboradores regulares do trabalho contínuo de pesquisa e desenvolvimento de políticas. Muitas vezes, fornecemos métricas e dados para ajudar a embasar as discussões da comunidade sobre temas específicos, como abuso do nome de domínio ou renovações de nomes de domínio de gTLDs.

Também analisamos propostas de textos de políticas e cláusulas de contratos. É claro que, sob o nosso ponto de vista, gostamos de ver coisas claras e aplicáveis. Isso facilita muito o nosso trabalho. Basicamente, quando estamos envolvidos nessas coisas, temos especialistas no assunto designados para qualquer desenvolvimento de política relevante que esteja acontecendo, dedicados a participar dessas sessões contínuas e fornecer

feedback. Isso leva muito tempo, mas estamos sempre felizes em participar.

Também estamos envolvidos em sessões de treinamento e divulgação. Muitas vezes, pode ser um encontro individual com as partes contratadas, conforme necessário, ou às vezes temos sessões de divulgação mais amplas da ICANN que são interdepartamentais, e geralmente participamos delas também ou quando solicitado. Aqui neste slide, vocês podem ver alguns dos projetos atuais dos quais participamos. ccPDP4, IDNs, implementação do EPDP Fase 2 e muito mais.

É claro que temos a página dedicada para métricas e painéis, que aproveitamos muito ao fornecer essas informações. Acho que isso é tudo. Vocês podem conferir aqui. Bom, agora temos tempo para perguntas e respostas. Não estou vendo nada no espaço de perguntas e respostas, então, se quiserem perguntar algo, a hora é agora. Estou vendo o Nigel. Você consegue ativar o microfone, Nigel?

NIGEL HICKSON Isso, sim.

JONATHAN DENISON Pronto.

NIGEL HICKSON Estão me ouvindo?

JONATHAN DENISON Claro. Sim, podemos ouvi-lo.

NIGEL HICKSON Muito bem. Bom, muito obrigado. Obrigado, Jonathan, e obrigado por todas as apresentações. Foram muito informativas e claras, e foi bom ver o que está acontecendo. Vai ser muito interessante ouvir os resultados da auditoria de registro. Minha pergunta volta ao início, pois foi muito revelador ver isso. Anotei alguns números, mas não estou achando. 204, será que era isso?

JONATHAN DENISON Está falando de abuso, Nigel?

NIGEL HICKSON Bom, é...

JONATHAN DENISON Posso voltar ao slide.

NIGEL HICKSON Sim, peço desculpas. Não quero tomar muito tempo.

JONATHAN DENISON Não se preocupe. Acho que é este aqui. Sim.

NIGEL HICKSON

Sim, isso mesmo. Então, vocês resolveram 204 investigações de mitigação, e isso resultou em apenas algumas notificações de violação e coisas assim. E você mencionou que, caso essas investigações pudessem ser resolvidas pelo registrador ou caso o registro tomasse as medidas adequadas, talvez derrubar os nomes de domínio, e você mencionou 2.900 nomes de domínio e a desativação de mais de 365 sites de phishing.

Então, a pergunta é a seguinte: imagine que eu sou um registrador e sou considerado culpado, mas tomo medidas imediatamente e resolvo o problema. Só que depois eu faço a mesma coisa. É claro que algumas vezes, eu posso conseguir escapar impune. Então, talvez haja outra denúncia da minha falta de conformidade ou do fato de que estou hospedando os sites duvidosos. Então, queria saber o seguinte: um registrador pode cometer um erro uma vez, mas se for pego em mais de duas denúncias em um ano, ou três ou quatro, o que vocês fazem nesse caso? Imagino que vocês não deixem por isso mesmo.

LETICIA CASTILLO

Obrigada, Nigel. Oi, sou Leticia Castillo. Ótima pergunta. Então, temos planos de remediação incluídos no sistema que fazem a sinalização e o monitoramento. Esses planos são necessários quando uma falha identificada afeta vários domínios ou sistemas além dos nossos processos, ou quando não existe um processo para resolver o abuso do DNS. E isso vai além de um caso

específico. E a causa raiz deve ser abordada para evitar a recorrência, que é o que você mencionou.

Então, por exemplo, temos um registrador... Acabei de me lembrar de um exemplo que admitiu que a equipe não estava preparada para lidar com uma denúncia. Eles ainda estavam aprendendo a lidar com denúncias de abuso do DNS e o caso não foi processado de forma adequada. Esse registrador nos apresentou um programa de treinamento como parte do plano de remediação, detalhando a duração do programa, os materiais usados, quem seria o condutor e como o sucesso seria medido.

O plano de implementação foi confirmado no final de outubro. E encerramos o caso. Agora, estamos monitorando novas denúncias e sinais de falhas recorrentes para esse registro específico. É cedo demais para definir se o plano foi totalmente efetivo, mas exigimos remediações detalhadas, documentadas no sistema e monitoradas. E uma falha recorrente no caso de uma questão resolvida anteriormente resulta em ações de conformidade aceleradas. Então, não passaremos pelo processo normal. Vamos expandir a questão e possivelmente emitir várias notificações de violação, que têm um impacto direto sobre o credenciamento das partes contratadas com a ICANN.

NIGEL HICKSON Muito obrigado.

JONATHAN DENISON Certo. Mais alguma mente curiosa? Caso contrário, passo a palavra a Jamie para o encerramento.

JAMIE HEDLUND Encerramento. Gostei. Obrigado, JD. Muito obrigado a todos. E obrigado por participar do webinar de hoje. Espero ver muitos de vocês em Seattle. Se virem a gente, podem parar e fazer perguntas ou dar ideias e sugestões. Se preferirem, também podem enviar um e-mail. Estamos sempre em busca de ideias sobre como trabalhar melhor e fornecer informações mais relevantes e úteis para todos. Agradeço pelo tempo de vocês. Boa viagem a todas as pessoas que vão a Seattle. Obrigado.

JONATHAN DENISON Obrigado a todos. Acho que já podemos interromper a gravação.

[FIM DA TRANSCRIÇÃO]