JOHANESBURGO – Sessão do GAC sobre a revisão da KSK
Quinta-feira, 29 de junho, 2017 – 12:00 às 12:30 JNB
ICANN59 | Johanesburgo, África do Sul

DAVID CONRAD: Implementado em 2010, quando fizemos a assinatura da Raiz pela primeira vez. Dissemos à comunidade que depois de cinco anos mudaríamos a chave. Isso é chamado como "rolar a chave". Agora, estamos em 2017 e estamos no processo de fazer essa mudança. Quando o Adobe decidir cooperar, eu vou mostrar alguns slides.

Nós fornecemos, enviamos uma carta aos regulamentadores de 180 países, e representantes desses países no GAC. E nesse documento queríamos alertá-los que haveria essa operação e para eles se preparassem para essa mudança. Então, essa é uma visão geral da zona raiz. Essa chave da zona raiz é criptografia mais elevada público/privada que tem duas partes. São as instalações de gestão da chave, um na costa leste dos Estados Unidos e outra na costa oeste. Foram estabelecidos em 2009 quando havia o contrato com o departamento de comércio Americano.

Nas instalações há um alto nível de segurança, uma sala segura dentro da sala segura, uma gaiola segura, um cofre onde estão

os módulos de segurança de hardware que são especializados na criptografia. E a chave privada dessa zona raiz é mantida dentro dessa sala segura.

A parte pública desse par de chaves é copiada e em cada resolutor do DNS que faz a validação do DNSSEC no planeta. Temos ao redor de 100 milhões de resolutores, e uma pequena percentagem, de fato, faz a validação do DNSSEC. Mas de qualquer forma, estamos falando de milhões de resolutores que têm essa informação.

A chave é usada no DNSSEC para construir uma cadeia de confiança desde a raiz do DNS até a folha da árvore que, na verdade, é o que está sendo visto na internet e garante que os dados que foram assinados pelo proprietário da zona, pelo DNSSEC, não será modificado.

Então, por que está havendo essa rolagem da chave? Em termos de melhores práticas de segurança, se você tem uma senha, você deve muda-la de vez em quando para evitar que ela seja comprometida sem seu conhecimento, e para garantir que a infraestrutura necessária para mudar a senha efetivamente funciona no caso de você precisar muda-la por qualquer razão. Isso também se aplica ao DNSSEC.

Então, essa assinatura na chave é uma senha para o DNSSEC, e como resultado, precisamos garantir que a infraestrutura que

existe para mudar a chave efetivamente funciona se houver a necessidade de mudar. Talvez, se houve uma tecnologia de ponta que permita a faturização...

O problema é que, levando em conta o número de dispositivos que existem, isso deve ser feito com muito cuidado e muito devagar. Preferimos que a internet não seja interrompida enquanto isso. É feito o problema, e se for cometido um erro durante essa operação, os resolutores, os servidores, as maquinas, os servidores usados pelos usuários finais que foram buscar o nome na internet, tudo vai parar de funcionar espontaneamente e vai ser muito ruim para todos.

Então, preferimos que isso não aconteça. Fazemos uma abordagem bastante cautelosa para garantir que não haja risco significativo e que não haja qualquer problema de validação do DNSSEC na internet. Esse é um processo que leva, mais ou menos, dois anos e meio.

São as datas que já ocorreram e em que irão ocorrer no futuro. No dia 19 de setembro o tamanho da chave foi aumentado. Tivemos que inserir a nova chave no DNS para seu uso nas chamadas cerimônias de chaves posteriores, que vão acontecer nessas instalações seguras.

Então, vão usar a chave privada e assinar a chave da (ininteligível). Isso é feito a cada trimestre. A ultima foi dia 24 de

setembro... na verdade 19 de setembro de 2007, então, o tamanho da chave será maior, porque será adicionada mais uma chave em 11 de outubro ela será usada pela primeira vez.

É uma data em que algo estranho pode acontecer, e com "estranho" eu quero dizer que aqueles que não mudaram sua chave até 11 de outubro, os resolutores não vão validar seus nomes de domínio em qualquer...

Então, nome de domínio buscado vai ter como resultado dizendo que o host não foi encontrado, ou erro 404. E no dia 11 de janeiro a chave antiga será revogada. 22 de março será o ultimo dia em que a chave antiga vai aparecer e, em agosto de 2018, ela será apagada.

Quem será afetado por isso? Os desenvolvedores de software de DNS e distribuidores, porque vão precisar da nova chave, integradores de sistema, que empregam os... quem emprega o software precisa garantir que ter essa nova chave, operadores de rede que em geral rodam os resolutores e precisam garantir que o seu sistema consiga dar suporte a essa alteração de chave. Operadores de servidor raiz. Porque esses provavelmente terão mais problemas se as chaves não foram mudadas. Geralmente, o que acontece é que vão tentar várias vezes resolver algo, e se falar a validação do DNSSEC, os provedores de serviço da internet que vão receber telefonemas se houve

algum problema se eles não atualizarem a chave, e os usuários finais serão afetados.

Então, obviamente é necessária muita preparação. Nós solicitamos aos operadores de rede se eles permitiram a validação do DNSSEC e, depois disso, ver se podem atualizar a chave. Em geral, os resolutores, historicamente, observaram que havia problemas em tentar mudar a chave. Então, o que os operadores de resolutores precisam fazer? Eles devem ver se o DNSSEC está autorizado em seus servidores. Ver se as coisas estão sendo escritas no lugar certo. E a validação deve ser permitida ou estar planejada no sistema.

Então, ter um plano para participar nesse Rollover da chave e saber o que pode dar errado. Por exemplo, um resolutor não atualizou a chave e vai começar a responder dizendo que o servidor falhou, etc.

Que pena. Essa caixa azul aí foi a carta que enviamos para os regulamentadores de cada país representantes do GAC para sugerir que falem com os operadores de rede de seus países para garantir que saibam que vai acontecer essa operação. Era isso que eu tinha que apresentar. Gostaria de responder qualquer pergunta e fornecer quaisquer informações que vocês queiram para informar os operadores de rede de seus países. Eu sou David Conrad, muito obrigado. Este é o meu e-mail.

CHAIR SCHNEIDER: Minha pergunta: existe algum número de telefone analógico de haver interrupção e que funcione 24 horas por dia, sete dias por semana?

DAVID CONRAD: O centro de suporte global da ICANN tem esse número.

CHAIR SCHNEIDER: Obrigado. Eu gostei muito da sua apresentação. Recebemos a sua carta e, para ser honesto, precisamos trabalhar com os nossos ISPs. Mas em termos de nos dar orientação, nós, como governo, precisamos fazer alguma coisa, não só garantir que nossos ISPs façam o que eles têm que fazer. Há alguma coisa que vocês recomendam que devamos fazer?

DAVID CONRAD: Bom, dentro de qualquer rede interna do governo é necessário haver Um resolutor em algum lugar. Pode ser externo. Por exemplo, o Google fornece seu serviço de DNS público, 8.8.8.8. Outros também utilizam esse serviço.

Então, todos precisam ser capazes de lidar com essa mudança de chave. O Google, eu certamente sei que ele pode fazer isso, mas outros ISPs, outras operações de rede, especialmente a

nível de empresa, é bom verificar que eles sabem que a chave vai mudar, e também permitir o funcionamento do DNSSEC. Se não souberem que a chave vai mudar, sugerir que participem das atividades que a ICANN tem publicado.

O que é importante, como já fiz em outras ocasiões, é fazer com que as pessoas saibam que isso vai ocorrer. Muitas vezes não conseguimos atingir a todos. Então, acho importante que os governos façam esse esforço para fazer com que todos sejam alertados que essa operação está ocorrendo.

CHAIR SCHNEIDER: Irã.

IRÃ: Há algum canal de feedback para garantir que a ação que você mencionou foi devidamente implementada antes de qualquer interrupção? Nem todos conhecem esse tema muito bem. Algum lugar que tenha um feedback, é bom recebermos a carta: “temos essa dificuldade”.

DAVID CONRAD: Em geral, nós estimulamos que as pessoas entrem em contato conosco para dirimir dúvidas. Nós não temos nenhum mecanismo explicito para receber o feedbaack, mas estamos

trabalhando em especial com vários operadores de rede, vários TLDs para criar canais de comunicação para esse feedback.

CHAIR SCHNEIDER: Egito, Noruega e Reino Unido.

EGITO: Obrigado Tomas, David, pela apresentação. Eu quero fazer uma pergunta sobre o slide número cinco. Se entendi bem, há alguma ferramenta para verificar que a pessoa está disponível?

DAVID CONRAD: Sim, criamos um banco de provas que permite aos operadores realizar uma prova em tempo real para entregar a chave. Isso não estava preparado porque está orientado em uma audiência mais técnica, mas podemos, talvez, passar essa informação ao GAC para que passem, por sua vez, às operadoras de rede em cada um dos países.

EGITO: Sim, isso seria muito útil. A outra pergunta que quero fazer é: isso vai impactar os resolutores? Porque não vejo aqui que estejam os ccTLDs; é apenas para os operadores de registro de TLD?

DAVID CONRAD: Bom, aqueles que vão receber as consequências são a parte do DNS que, na verdade, toma informação dos operadores dos TLDs. Os ccTLDs e gTLDs não vão receber impacto pelo fato de transpassar a chave, porque não tem nada a ver. Não é uma funcionalidade que eles ofereçam. São os operadores de rede os que receberão os impactos, e também os resolutores.

PAÍSES BAIXOS: Obrigado, David, pela apresentação. Quero verificar algumas questões. Eu acho que os governos não vão ter uma responsabilidade formal, mas os senhores estão fazendo difusão externa para contatar os ISPs, mas não há uma responsabilidade governamental.

DAVID CONRAD: Correto.

PAÍSES BAIXOS: Em segundo lugar, houve uma lista dos resolutores recursivos de DNSs, eles são a avaliação do DNS. Acho que serão contatados diretamente, porque são aqueles que tem que fazer a mudança real em seu sistema, não? E também, há outras partes interessadas que vão receber o impacto. Mas tem que mudar os seus sistemas?

DAVID CONRAD: A forma na qual vai se realizar o processo de transpasso de chave é de forma automática. Caso se trate de um operador resolutor e tem o seu board atualizado, então não tem que fazer nada. Talvez devam ser prudentes e participar nos bancos de prova para ter certeza de que nada estranho vai acontecer quando se realize o transpasso. Mas, é um sistema automatizado dentro desses resolutores que ajuda a fazer a passagem de forma automática.

Se não tem o software atualizado, ou se não ativaram a passagem automática, então vão ter que mudar a configuração do ponto de dados. Na verdade, isso está associado com a KSK. Isso terá que ser copiado em um arquivo de configuração. Estes seriam os casos nos quais os operadores de resolutores teriam que fazer alguma coisa.

CHAIR SCHNEIDER: Passo a palavra ao Reino Unido.

REINO UNIDO: Obrigado, David, por essa apresentação. Ainda não falei com os membros da unidade constitutiva das ISPs e ISPC, mas eu suponho que os senhores vão falar com eles para fazer difusão externa com eles. Eu suponho também que isso está

funcionando dessa forma. Eu não vi a carta, deveria ler e verificar o conteúdo, de que forma finalmente ficou redigida. Eu também acho que é uma coisa que deveríamos verificar, porque falou dos fornecedores de redes governamentais... o que eles vão fazer em 11 de outubro?

Estamos todos prestando atenção nessa data. Se alguma coisa der errado, haverá alguma pedida de proteção? Como vão abordar as falhas importantes que podem surgir nessa data?

DAVID CONRAD: Sim. Nós entramos em contato com as ISP e ISPCP e incentivamos para que entrassem em contato com outros organismos semelhantes. A respeito ao que aconteceria se acontecer algo de errado: nós estabelecemos o sistema de observação muito elaborado para monitorar os tráfegos dos servidores raízes, que seriam a primeira indicação de que há algo de errado. Temos um plano de contingência que poderia ser implementado caso detectemos alguma espécie de evento significativo, caso exista alguma falha na passagem da chave. Nós estamos bastante confiantes de que provavelmente os governos possam receber alguns comentários dos usuários e operadores de rede.

Por esse motivo, estamos trabalhando para que a informação chegue de forma correta para que todos tenham a senha atualizada.

CHAIR SCHNEIDER: Por favor, não vão embora. Há um anuncio que farei daqui um minuto que é importante. Quero passar a palavra para um senhor que está lá atrás, da Nigéria. Por favor, não vão embora. Essa é a ultima intervenção, depois teremos que finalizar.

NIGÉRIA: Obrigado pela apresentação sobre a passagem.

A minha pergunta é a seguinte: para os operadores, ou para fornecedores de servidores de rede que não habilitaram o DNSSEC, o que vai acontecer depois da passagem?

DAVID CONRAD: Não vai haver nenhuma mudança. Se não habilitaram a DNSSEC, a passagem da chave não vai ter qualquer impacto. Se em algum momento futuro decidem habilita-la, terão que ter certeza que contarão com a chave atualizada. Caso contrário, a avaliação vai falhar e vão se confundir. Tem que atualizar a chave, ou ter o software de distribuição atualizados para poder receber uma atualização automática.

CHAIR SCHNEIDER: Vamos ter que parar aqui, mas eu quero fazer um comentário breve. Sendo que temos uma coisa importante para contar, como os senhores sabem, esse é o nosso último almoço nessa reunião. Também é o último almoço para Olof em seu cargo. Quando seu cargo, na verdade? É do pessoal da ICANN que dá apoio, o GAC, e que sempre faz piadas e ligações durante a noite. Então, seu apoio é necessário.

Então, Julia, que talvez esteja escondida lá a trás – saiu – nos ajudou a organizar um pequeno presente para Olof. Vamos verificar com o pessoal técnico de que forma ele pode levar até seu lar. Esse é o presente, esse é o cartão... não é muito pesado, então vai poder levar. Basicamente, queríamos, mais uma vez, dizer: Olof, obrigado.

Há algumas taças lá atrás e algumas coisas para comer e comemorar os últimos momentos de Olof em seu cargo. Muito obrigado, Olof.

OLOF NORDLING: Muito obrigado. Eu sempre quis um presente assim. Realmente, muito obrigado. Espero continuar em contato. Inclusive, embora eu me retire, estarei aqui até finais de julho. Então, não vão se

livrar de mim tão facilmente. Pelo menos não por enquanto. Obrigado.

BRASIL: Tomas, uma pergunta: depois do almoço nós vamos nos reunir aqui novamente, mas qual o objetivo? Acho que deve ter de novo o comunicado ou não será necessário? Como vamos fazer? Ontem falamos de nos reunirmos pelas três horas...

CHAIR SCHNEIDER: Vamos ver o texto que já temos. Tom estava trabalhando, vamos analisar durante o almoço. Mas a ideia seria que três horas possamos ter tudo pronto e dedicar apenas alguns minutos para poder finalizar. Mas obrigado por relembrar. Não vão embora ainda, não terminamos de trabalhar.

Em primeiro lugar, não é o trabalho. Vamos comemorar com o Olof.

[FIM DA TRANSCRIÇÃO]