САН-ХУАН — Отчет об обновлении KSK
Среда, 14 марта 2018 года, 16:15–16:45 по AST
ICANN61 | Сан-Хуан, Пуэрто-Рико

НЕИЗВЕСТНЫЙ ДОКЛАДЧИК: Приветствую всех, совсем скоро мы начнем заседание на тему обновления ключа для подписания ключей (KSK) корня. Выведите, пожалуйста, презентацию на экран.

Мы начинаем через 30 секунд.

Приветствую всех на заседании, посвященном обновлению KSK корня. Надеюсь, что присутствующие в зале еще не видели мое выступление на данную тему на этой конференции. Итак. Начну с краткого пересказа событий, предшествующих сегодняшнему положению дел. Думаю, все заинтересованные в данном вопросе в достаточной мере для того, чтобы присутствовать в зале, знают, что обновление KSK корня изначально было запланировано на 11 октября 2017 года, но мы решили это мероприятие отложить. [Неразборчиво] проанализировали нашу отчетность о якоре доверия CAD 145. Они обнаружили, что у 7–8% всех резолверов, от которых поступали сообщения — на тот момент это была относительно небольшая цифра, — был только так называемый KSK 2010 или текущий возвратный KSK и не

было нового KSK корневой зоны. Что-то с этими 7–8% было не в порядке. Исследовательская группа офиса технического директора (CTO) Интернет-корпорации по присвоению имен и номеров (ICANN) провела такой же анализ трафика с различных корневых серверов, и мы пришли, по сути, к тому же выводу. В зависимости от точного времени анализа, эта доля выше или ниже. Всё равно эта доля была выше приемлемого для нас значения, и, что более важно, мы не понимали причины, по которой от этих резолверов поступали сообщения о старом ключе. Мы решили приостановить обновление KSK корня и попробовать разобраться в том, почему у этих резолверов старый ключ. Мы взяли список из 500 резолверов, от которых в сентябре 2017 года поступило сообщение только о старом ключе, только о KSK 2010, попробовали их отследить, и выяснилось, что отслеживание операторов по одному только адресу интернет-протокола (IP-адрес) — трудная задача. Мы это знали и получили тому подтверждение. Мы можем наладить контакт только с 20% — это около 100 адресов. Из них большинство относилось к IP-диапазонам, известным тем, что в них размещаются эфемерные объекты, такие как виртуальные машины и контейнеры.

Еще есть вопрос, касающийся запроса комментариев (RFC) 8145, состоящий в том, что сам сигнал отправлен как запрос системы доменных имен (DNS). Это означает,

что совершается, например, пересылка с одного резолвера на другой. Мы знаем, что имела место пересылка, скрывающая сигнал. Можно предположить, что конкретный резолвер имеет только KSK 2010 — он в порядке, а всё дело в предыдущем резолвере, с которого на первый идет пересылка, и это от него поступает сообщение только о KSK 2010.

Вывод здесь в том, что единственной явной причины не было. Прекрасно было бы обнаружить одну или две причины в корне. Мы могли поговорить с поставщиками и исправить ошибки, если бы их нашли, могли изменить свое сообщение, но так не получилось. Поскольку в результате исследования не сложилось четкой последовательности дальнейших действий, корпорация ICANN решила обратиться к сообществу.

Мы подошли к концу декабря 2017 года. Мы сказали, что примем предложения и дискуссию на тему обновления KSK через лист рассылки корпорации ICANN, посвященный новостям и обсуждению данного проекта. Если вы не подписаны на этот лист, предлагаю подписаться. На данный момент информации там немного, но [неразборчиво] с проектом. По результатам обсуждения сложилось общее согласие насчет того, что нет подходящего показателя для измерения. Прошло более двух лет с тех пор, как собранная ICANN группа разработчиков составила отчет об обновлении

возвратного KSK и дала рекомендации. Там говорилось, что хорошим показателем было бы количество пострадавших пользователей и что если после обновления KSK доля пострадавших пользователей составляет 0,5%, то это признак наличия достаточно серьезных проблем для совершения отката. Количество пользователей — показатель логичный, но очень трудный, и данные RFC 8145 свидетельствуют о другом. Среди людей бытовала надежда на появление в будущем лучших показателей. Надежды возлагались на некий проект, который сейчас называется Sentinel — это проект, над которым работает Уоррен Кумар (Warren Kumar) из Google и [неразборчиво], позволяющий производить измерения, ориентируясь на пользователей. Но это пока остается проектом. Группа пришла к консенсусу в том смысле, что ICANN должна своевременно обновить ключ и продолжать информирование, которым мы занимались.

На основании отзывов от 1 февраля мы опубликовали предварительный — именно предварительный — план обновления KSK. Согласно этапам плана, сначала мы собираемся отложить обновление на 1 год, перенеся его на 11 октября 2018 года. Мы надеялись, что в результате обсуждения через список получится сформулировать критерии измерения. Определенных критериев никто не предлагал. Мы также собираемся продолжить информирование, путем таких мероприятий как это

заседание, публикация сведений об обновлении KSK, и собираемся опубликовать дополнительные наблюдения в отношении данных о якоре доверия, в основном данных RFC 8145, хотя с каждым днем я всё больше и больше сомневаюсь в том, что можно из этих данных почерпнуть. Если из них можно почерпнуть что-то действительно полезное или просто получить тревожный сигнал, то это не особо важно для проекта.

Важный момент здесь в том, что у нас открыт период общественного обсуждения. Данный план — предварительный, и предложения сообщества приветствуются. Мы очень хотим услышать мнения сообщества и получить отзывы о предложении. Период общественного обсуждения заканчивается 2 апреля. Внизу страницы указан унифицированный адрес (URL) страницы с пояснениями. Если мы будем следовать текущему плану и расписанию, то с предварительным планом всё будет как-то так. Период обсуждения заканчивается 2 апреля. В середине апреля нужно будет опубликовать отчет персонала, как и при любом периоде общественного обсуждения ICANN. Мы внесем в план все необходимые изменения и опубликуем результат. Если вы знакомы с периодичностью заседаний Правления ICANN, оно собирается 6 раз в год, оно собирается на каждой конференции ICANN, так что 3 раза. Еще между конференциями ICANN оно проводит так называемый

семинар Правления, на котором собирается. Следующее заседание Правления ICANN состоится в середине мая, это будет семинар. На нём мы попросим Правление составить резолюцию с просьбой к ASAC и нашему SAC — я не обновил слайды — рассмотреть и прокомментировать план к 1 октября. Вероятно, состоится еще одно заседание в Панаме, на котором будет обсуждаться обновление KSK корня. Мы надеемся 1 октября, получив отзывы ASAC и наших SAC, внести в план все необходимые изменения. Если в результате этих изменений не потребуется переориентироваться с 11 октября 2018 года на другую дату, то к середине августа мы опубликуем итоговый план, а на семинаре в сентябре попросим Правление составить резолюцию с указанием корпорации ICANN обновить ключ 11 октября.

Таково положение дел и дальнейшие планы на сегодняшний день. Опять-таки невозможно выразить, как нам нужны мнения сообщества и участие людей в общественном обсуждении. Я бы хотел отправить остальную часть презентации, про получаемые нами сигналы, про данные, получаемые посредством сообщений якорей доверия RFC 8145.

На сегодняшний день офис технического директора ICANN имеет доступ к данным RFC 8145 через... Собственно говоря, этот слайд устарел, судя по новым сведениям от 12 корневых серверов, мы внесли сервер H

в перечень серверов, от которых получаем данные. В первоначальном анализе в конце 2017 года использовались [неразборчиво] данные серверов B, D и F, но с тех пор мы используем [неразборчиво] надстройку для предела DNS. Операторы корня работают с пределом DNS, трафик анализируется в реальном времени и каждые 60 секунд эта надстройка составляет статистический отчет на основании того, что увидела, и на основании увиденных ею сообщений якорей доверия. Она отправляет им DNS-запросы — довольно умный ход, — в зону, с которой ICANN [неразборчиво] работает. Перед вами примеры того, как выглядят эти сообщения: вот временная метка, вот исходный IP, разделенный дефисами, а не точками. Якори доверия записаны шестнадцатеричным номером из четырех цифр: 4A5C — это KSK 2010, 4F66 — это KSK 2017. Далее вы видите идентификатор примечания и идентификатор корневого сервера. На основании всей этой информации мы можем составить данный график. Как видите, с течением времени мы получаем всё больше сообщений от дополнительных серверов. Я дам пояснения к этому графику, поскольку с первого раза он может быть не вполне понятен. Тремя линиями изображены две вещи. Красная и зеленая линии соответствуют количеству IP, от которых поступают сообщения о данных 8145, и их можно увидеть на оси слева — количество источников. Как видите, с течением времени... Взгляните на зеленую

линию — это текущее общее количество источников, от которых поступают сообщения о данных якорей доверия. Это уникальные источники за день. На сегодняшний день к нам ежедневно поступают сообщения о данных якорей доверия приблизительно от 50 000 уникальных IP-адресов. Красная линия соответствует количеству тех, которые сообщают о наличии у них только старого ключа. Если разделить красную линию на зеленую, то получается процентное отношение, которому соответствует черная линия. Этот масштаб представлен на оси Y справа. Как видите, сейчас примерно от 20% резолверов нам поступают сообщения о том, что у них только старый ключ. Обратите внимание на большой скачок в январе, когда внезапно намного больше людей стали отправлять сообщения, а процентное отношение стало хуже. Мы с высокой долей уверенности можем утверждать, что причиной этого было обновление Unbound. Сервер Unbound 168 был запущен в середине января, так что по времени всё сходится. Целью этого запуска было решение проблем безопасности, уязвимости системы. Мы считаем, что, поскольку это обновление связано с безопасностью, люди были мотивированы обновить Unbound. Однако, после 30 дней количество сообщений о KSK 2010 не уменьшилось.

Если обновить Unbound и не запустить якорь Unbound... Я скажу по-другому: если обновить Unbound и запустить

якорь Unbound, то якорь доверия сразу же обновится, получит нужные данные и будет работать как с KSK 2010, так и с 2017. Нередко при обновлении якорь Unbound не запускают, и это означает работу с версией Unbound, настроенной со старым ключом. Но если RFC 5011 выполняется как надо, то через 30 дней он должен провести этот процесс и понять, что KSK 2017 тоже нужно настроить. Почему этого не произошло? Одна из возможных причин состоит в эфемерных виртуальных машинах или контейнерах. Представьте себе, что появляется нечто подобное со старым ключом, сообщает о старом ключе посредством RFC 8145... Я говорю «старый ключ», а надо говорить только «KSK 2010». Сообщает о KSK 2010, работает несколько часов, несколько дней, выключается. У него нет времени выполнить RFC 5011 [неразборчиво] при следующем запуске, он начинает заново и по-прежнему работает только с KSK 2010, сообщает только о KSK 2010 посредством 8145, и данный процесс повторяется. На каком-то этапе мы должны провести дальнейший анализ, необходимо перестать работать над своими слайдами, отправиться в Пуэрто-Рико и представить их — это мы сейчас и делаем. В числе прочего, мы должны отслеживать конкретные IP, как часто они имеют место, как часто поступают сообщения. Мы знаем, что серверы BIND и Unbound отправляют сообщения 8145 довольно регулярно. Если мы видим, что какие-то IP этого не

делают, то резонно предположить, что они [неразборчиво] поднимаются и падают. Это не единственная возможная причина, но поэтому мы и проводим исследование, пытаясь разобраться.

Вот графики индивидуальных корневых серверов. Эти графики одинаковые, поскольку этот график соответствует всем корневым серверам, а вот эти графики соответствуют корневым серверам — их на тот момент было 11, — откуда мы получаем данные. Вы видите данные, серверы, от которых мы получаем данные, в различные периоды времени. Эти графики относительно схожи, за исключением корневого сервера J, для которого процентное отношение сообщений ниже. Так что у корневого сервера J ситуация выглядит получше, чем у остальных. Если говорить о процентном отношении, во всяком случае. [Неразборчиво] сообщения, что мы получаем сообщения не от всех зеркал корневого сервера J, так что это тоже, возможно, имеет значение в данном случае. Суть здесь в том, что данные по корневым серверам не слишком различаются между собой. Мне кажется интересной смена поведения, произошедшая в середине января, когда был скачок. На этом графике показано количество уникальных IP-адресов, появляющихся каждый день. Эта величина показывает, от скольких источников в тот или иной день нам поступили данные, которых мы ранее не видели.

Если взглянуть на значения слева направо, то они у нас составляли, похоже, не более 1000, несколько сотен новых IP каждый день. После предполагаемого обновления в январе мы внезапно видим гораздо больше уникальных источников в день, от которых поступают сообщения. Около 15 000–16 000. Если бы пришлось составить график с количеством накапливающихся уникальных IP, которые мы видим каждый день, то он выглядел бы так. Зеленая линия соответствует количеству зафиксированных нами IP-адресов в любой момент времени. Очевидно, что вначале, раньше, слева эта цифра маленькая, и чем больше проходило времени, тем больше мы видели уникальных IP-адресов. Сейчас их число составляет 730 000. На сегодняшний день у нас было 730 000 разных IP-адресов. Я не говорил в презентации, что там есть адреса как 4-й версии (V4), так и 6-й (V6). Нам поступили сообщения примерно от 730 000, из которых около 250 000 в разное время сообщали, что у них есть только KSK 2010. Если взглянуть на количество, накопившееся у нас на сегодняшний день, то в этом расчете цифры еще хуже. Из всех виденных нами адресов приблизительно 35% сообщили только о KSK 2010.

Я решил рассмотреть эту информацию через /24, и, как видите, форма этого графика немного отличается. После увеличения в январе был скачок новых /24, а затем

небольшое снижение. Но если очерчивать процесс накопления, то у нас всё равно много /24. Если взглянуть на зеленую линию, то наибольшее значение составляет приблизительно 350 000. Таким образом, мы имеем среднее значение — сильно теряем в разрешении — около 2 IP на /24. Я надеялся, что эта цифра будет меньше и укажет на то, что, возможно, были блоки с целой кучей адресов, и мы могли бы их изучить. На этот случай была бы хорошая гипотеза, заключавшаяся в том, что были поля адресов с одними лишь динамическими эфемерными машинами.

Это большое количество адресов. Интересно, что в общем количестве адресов, с которых поступали сообщения о KSK 2010 или о KSK 2010 и KSK 2017, эта цифра была больше общего числа уникальных IP. Это означает, что существуют источники, сообщившие о наличии KSK 2010, а затем сообщившие о наличии KSK 2010 и KSK 2017. Необязательно в таком порядке, но они передали оба сообщения. Вот одна из причин, по которым это может произойти. Представьте себе источник, сообщающий о KSK 2010, а позднее — о KSK 2010 и 2017. Одна — не единственная — из возможных причин состоит в том, что машина обновила ключ. Теперь у нее новый KSK, но из 750 000 IP всего около 1550 сообщают о двух. Это означает, что невелико количество машин, в отношении которых мы можем сказать, что одна из

гипотез — они были обновлены. Часть проблемы здесь в том, что существуют трудности с сигналом 8145. Мы знаем, что в процесс вовлечены передаточные элементы, как я и упоминал, и сообщение от IP-источника не является гарантией того, что вы видите конфигурацию именно этого IP-источника. Возможно, кто-то еще передает сообщение 8145 с описанием своей конфигурации на этот IP, который затем отправляет его на корневой сервер, и мы его видим. Это еще одно объяснение того, почему мы видим от одного источника сообщение о KSK 2010 и о KSK 2010 и 2017.

Мы также знаем о существовании как минимум одной версии реализации, в которой отправляется сообщение 8145 даже при отсутствии проверки правильности. Если бы у нее был KSK 2010, это не имело бы значения, поскольку она осуществляла проверку правильности DNS и использовала этот элемент как часть своей конфигурации. Ее соответствующим образом настроили, но это было неважно.

Если хотите ознакомиться с этими графиками самостоятельно, то мы еженедельно их обновляем. Вот их URL. Root trust anchor reports, точка, ICANN, точка, org. Я только начал анализировать данные таким образом, он основан конкретно на этой таблице, не основан на всех 250 000 IP, которые на данный момент сообщили только о KSK 2010. Это основано на меньшем количестве, и я

навскидку не помню, каким было общее число. Здесь за основу берется количество источников на автономную систему, затем осуществляется своего рода обратное действие, чтобы номера автономных систем (ASN) с наибольшим количеством IP, отправивших сообщения... Прошу прощения, это не только KSK 2010, это все номера автономных систем, откуда поступили сообщения. Если речь только о KSK 2010, то график выглядел бы по-другому. Это означает, что мне нужно провести данный процесс еще раз, ориентируясь только на KSK 2010, и мы сможем попытаться выяснить, как обстоят дела с автономными системами (AS) с наибольшим количеством резолверов, сообщающих только о KSK 2010.

Мы распространили список IP-адресов, которые сообщили Группе интересов интернет-провайдеров и провайдеров связи (ISPCP) и RAR только о KSK 2010, и цель двойная. Во-первых, конечно, обновить системы. Но нам также очень интересно узнать, что происходит и почему эти системы не обновляются. Если мы обнаружим, например... Один из лучших возможных результатов — выявить существование адресного пространства, на котором группа [неразборчиво] машин, которые работают по старой конфигурации, только с KSK 2010. Это был бы положительный результат. Этот слайд устарел, власть имущие в ICANN позволили мне обеспечить общий доступ к списку. Мы опубликуем

страницу, это будет выглядеть вот так. Я отсортирую ее в обратном порядке по ASN, и вы сможете выбрать ASN и получить список адресов от этого ASN, от которых поступили сообщения о KSK 2010. Скоро операторам будет гораздо легче выяснить, что происходит в их сети. Конечно, тогда мы будем связываться с операторами, начиная с тех, у кого больше всего сообщений только о KSK 2010, и пытаться выяснить, что происходит. Дальнейшие действия: будем продолжать пытаться выяснить, как обстоят дела с данными 8145. Я не доволен теми сигналами, которые они дают, но пока других данных у нас нет. Важно продолжать исследования, пытаться выяснить, что мы можем почерпнуть. Если на каком-то этапе мы будем убеждены, что никакой ценной информации не получаем, то это само по себе — тоже положительный результат. Мы попробуем связаться с сетями, от которых поступают сообщения о большом количестве резолверов только с KSK 2010, поможем другим провести исследования. Мы продолжим это обсуждать, так что вы будете видеть меня и моих коллег, и мы будем и далее прислушиваться к сообществу, поскольку, как я сказал, существуют пути, которыми вы можете помочь: комментируйте план, опять-таки есть URL, и, пожалуйста, подписывайтесь на лист рассылки по обновлению KSK, чтобы быть в курсе событий. Теперь я с радостью отвечу на любые вопросы. У нас есть немного

времени до следующего мероприятия, которое начнется здесь в 17:00.

ГОВАРД БЕНН (HOWARD BENN): Это Говард Бенн из Samsung Electronics. На том слайде, где у вас были все операторы — вот этот. Предполагаю, что сеть Reliance Jio — наверное, их LTE-сеть работает полностью на виртуальных машинах, и практически нет сомнений, что она не уложится в 30 дней. Существует множество операторов мобильной связи. Будет очень интересно посмотреть, столкнутся ли все они с теми же проблемами. Опять-таки я с радостью предоставлю контактную информацию по Jio, поскольку это оборудование — наше.

НЕИЗВЕСТНЫЙ ДОКЛАДЧИК: Хорошо, спасибо.

МАРК (MARK): Марк [неразборчиво] с интернет-провайдерами (ISP), но здесь выступаю от своего имени. Можем перейти к слайду 4? Да, этот. Я смотрю на нижнюю часть слайда, где говорится о результатах обсуждения. Здесь же один в трех. Я изложу их своими словами, а вы скажете мне, правильно ли я всё понял. В первом пункте говорится, что мы не знаем, какими будут последствия для интернета. В

третьем пункте говорится, что всё равно надо это сделать. Я правильно прочитал?

НЕИЗВЕСТНЫЙ ДОКЛАДЧИК: Это всё равно что говорить о стакане как о наполовину пустом.

МАРК: Можете подать информацию так, чтобы он был наполовину полон?

НЕИЗВЕСТНЫЙ ДОКЛАДЧИК: По-моему, остальная часть презентации говорит о том, что стакан наполовину полон. Я отвечу серьезно. Серьезный ответ состоит в том, что трудно знать, как поступить. Когда настала прошлая осень, мы решили, что нам необходимо вовлечь сообщество и получить его предложения. Ваше резюме — это то, что сказало нам сообщество. Отмечу, что выбор участников обновления KSK — это своего рода самоотбор. Это обычно люди, выступающие в поддержку расширений безопасности системы доменных имен (DNSSEC), имеющие личный капитал, знающие, что еще вложено в DNSSEC, и желающие успешного обновления. Наверное, если оглянуться, то неудивительно, что мы услышали такие мысли, но именно поэтому общественное обсуждение столь важно — оно дает нам

возможность посвятить в вопрос более широкую аудиторию, и если люди видят ситуацию как наполовину пустой стакан, то могут ее прокомментировать.

МАРК: Спасибо за разъяснение, я ценю его. В данном случае я всё равно вижу стакан наполовину пустым. Я считаю себя сторонником DNSSEC, поэтому не могу смириться... Я дам индивидуальные комментарии. Я не могу смириться с пунктами 1 и 3. У меня вызывает когнитивный диссонанс тот факт, что кто-то всерьез предлагает внести в корень изменения, последствия которых неизвестны. Я согласен с вами и полностью доверяю вашему анализу в отношении такого вот низкого качества получаемых сигналов, но с течением времени сигналы, которые вы получаете, — единственная имеющаяся диагностическая информация — становятся только хуже. Таково мое видение ситуации. Все слайды, которые идут после этого, я нахожу весьма убедительными, но вот этот слайд и пункты 1 и 3 из результатов обсуждения не укладываются у меня в голове. Не знаю, как кто-либо из технического сообщества мог сказать: «Давайте, вносите изменения в корень, не зная, к каким это приведет результатам». Спасибо. Я также подам эти комментарии индивидуально.

НЕИЗВЕСТНЫЙ ДОКЛАДЧИК: Я бы хотел озвучить, как можно это интерпретировать по-другому. Это не моя интерпретация, я просто повторяю услышанное. Суть в том, что у воздержания от обновления ключа свои отрицательные стороны. Это может стать причиной недоверия к ключу, даже при отсутствии ему прямой криптографической угрозы. Будь то угроза самой картографии или физической операционной безопасности ключа. Тем не менее, воздержание от обновления ключа может пошатнуть доверие к нему, а в сочетании с верой в то, что всё не так уж плохо и люди смогут его исправить, и вы принимаете неизбежность каких-то неполадок — соединив все эти факты, начинаешь верить, что ключ следует обновить.

МАРК: Если я понимаю такого рода доводы о репутации правильно, то мы хотим обновить ключ потому, что нам нужно доверие со стороны людей к DNSSEC. Я понимаю ту часть, которая касается репутации. С другой стороны, если догадки людей неверны — и я шокирован тем, что всё сводится к догадкам, — и всё будет хуже, чем мы себе представляли, то нам придется осуществлять откат. Пока в реальности у нас такого не было. По-моему, у нас будут проблемы с репутацией в обоих случаях. Таким образом, ICANN оказывается в трудном положении, и я это понимаю, но не убежден, что вопрос репутации с DNSSEC

равнозначен реализации с неизвестным результатом в октябре. Спасибо.

НЕИЗВЕСТНЫЙ ДОКЛАДЧИК: Еще вопросы или комментарии? Кэти (Cathy), есть что-то из интернета?

НЕИЗВЕСТНЫЙ ДОКЛАДЧИК: Нет.

НЕИЗВЕСТНЫЙ ДОКЛАДЧИК: О, да.

НЕИЗВЕСТНЫЙ ДОКЛАДЧИК: Спасибо за презентацию. Мой вопрос в следующем. Мы обнаружили... В Нигерии четыре мобильных сетевых оператора и большое количество ISP. Мы обнаружили, что лишь один из четырех поставщиков услуг мобильной сети использует DNSSEC — остальные три мобильных оператора [неразборчиво], отличные от DNSSEC. Каковы преимущества DNSSEC по сравнению с другими системами проверки безопасности? Если ли необходимость другим [неразборчиво] переходить на DNSSEC? И третий вопрос: что [неразборчиво] поставщикам услуг сети, использующим после

обновления KSK другую систему проверки? Огромное спасибо.

НЕИЗВЕСТНЫЙ ДОКЛАДЧИК: Не могли бы вы повторить последнюю часть вопроса?

НЕИЗВЕСТНЫЙ ДОКЛАДЧИК: Да, последнюю часть вопроса, пожалуйста.

НЕИЗВЕСТНЫЙ ДОКЛАДЧИК: Последняя часть вопроса касалась того, что три поставщика услуг мобильной сети не используют для проверки DNSSEC. Каковы тогда их [невнятно] после обновления KSK?

НЕИЗВЕСТНЫЙ ДОКЛАДЧИК: Прошу прощения, каковы их что?

НЕИЗВЕСТНЫЙ ДОКЛАДЧИК: Их [неразборчиво]. Будут ли какие-то последствия для пользователей?

НЕИЗВЕСТНЫЙ ДОКЛАДЧИК: Это легкий вопрос. Если проверка DNSSEC не проводится, то последствий обновления KSK

не будет никаких. Согласно позиции корпорации ICANN, проверка DNSSEC — это хорошо, так что мы призываем людей проводить проверку DNSSEC. Извините, но теперь я не помню первую часть вашего вопроса.

НЕИЗВЕСТНЫЙ ДОКЛАДЧИК: Первая часть моего вопроса звучала так: Каковы преимущества перехода к DNSSEC для тех, кто ими не пользуется?

НЕИЗВЕСТНЫЙ ДОКЛАДЧИК: Согласно позиции корпорации ICANN, проверку DNSSEC следует выполнять, поскольку без проверки DNSSEC не гарантируется, что получаемый ответ действительно отвечает на заданный вами вопрос и что он действительно поступает от того, от кого вы думаете. Нет криптографической гарантии того, что получаемые вами ответы действительно поступают оттуда, откуда поступают. Благодаря DNSSEC вы знаете, что ответ поступает от того, от кого говорится, и что с момента подписи он не меняется. Современные резолверы очень умны во избежание обмана, но в конечном итоге для более надежной гарантии необходимы DNSSEC. Без DNSSEC вы в определенной степени уязвимы для подмены, обмана или веры ответам, не соответствующим истине.

НЕИЗВЕСТНЫЙ ДОКЛАДЧИК: Большое вам спасибо.

НЕИЗВЕСТНЫЙ ДОКЛАДЧИК: Другие вопросы? Тогда спасибо вам за то, что пришли.

[КОНЕЦ СТЕНОГРАММЫ]