ЙОХАННЕСБУРГ - Заседание GAC по процедуре обновления KSK
Четверг, 29 июня 2017 года – с 12:00 до 12:30 JNB
ICANN59 | Йоханнесбург, Южная Африка

ПРЕДСЕДАТЕЛЬ SCHNEIDER: Итак, перед обеденным перерывом у нас есть еще одно заседание, которое касается процедуры обновления KSK. Важная информация, которую ICANN хотела разделить с нами, и здесь у нас есть Дэвид Конрад (David Conrad), который представится через несколько секунд и расскажет нам, почему он здесь.

НЕИЗВЕСТНЫЙ ВЫСТУПАЮЩИЙ: (Выкл. микрофон).

ПРЕДСЕДАТЕЛЬ SCHNEIDER: Да, да, просто займите любое место, или вы также можете прийти сюда в середину, Дэвид.

DAVID CONRAD: Привет всем, я Дэвид Конрад (David Conrad), технический директор ICANN, и я здесь, чтобы поговорить с вами о процедуре обновления подписания ключа, которую мы сейчас проводим. Подписание ключа - это ключ, который мы используем в DNSSEC, чтобы подписать что-то, называемое

Примечание. Следующий документ представляет собой расшифровку аудиофайла в текстовом виде. Хотя расшифровка максимально точная, иногда она может быть неполной или неточной в связи с плохой слышимостью некоторых отрывков и грамматическими исправлениями. Она публикуется как вспомогательный материал к исходному аудиофайлу, но ее не следует рассматривать как аутентичную запись.

ключом подписания зоны. Затем ключ подписания зоны используется для фактического подписания корневой зоны. Именно так осуществляется DNSSEC. И в 2010 году, когда мы впервые подписали корневую зону, мы сказали сообществу, что через пять лет мы изменим ключ, и это называется процедурой обновления ключа.И теперь это 2017 год, и мы сейчас проводим это изменение. Поэтому, как только Adobe заработает, у меня будет несколько слайдов, чтобы вам показать.

Это общая информация не вдаваясь в подробности, чтобы вы поняли. Мы представили письмо регулирующим органам, по-моему, 180 стран и национальным доменам, представителям GAC для тех стран, где это необходимо. И в этом письме мы намеревались просто предупредить регулирующие органы о том, что скоро пройдет обновление ключа и что они должны спросить у своих сетевых операторов, готовы ли они к этому изменению.

Итак, обзор. Таким образом, подписание ключа DNSSEC корневой зоны является самым верхним криптографическим ключом, который используется для защиты данных в DNS. Он состоит из открытой части и закрытой части. Частная часть хранится в так называемых защищенных дата-центрах. Их два. Один на Восточном побережье США и второй на Западном побережье США

Они были созданы еще в 2009 году, когда у нас был контракт с Министерством торговли США. Внутри этих центров есть - довольно высокий уровень безопасности. Там есть защищенный зал. В защищенном зале есть защищенная клетка. Внутри защищенной клетки есть сейф. И внутри сейфа есть так называемые аппаратные модули безопасности. Это специализированные устройства, которые содержат криптографическую информацию. Таким образом, закрытый ключ для корневой зоны содержится внутри этого - этого HSM (аппаратного модуля безопасности), внутри сейфа, внутри клетки, внутри защищенного зала, внутри помещений совместного доступа, которые имеют контроль доступа.

Открытая часть этой пары открытых/закрытых ключей фактически копируется в каждый DNS-преобразователь, который выполняет проверку DNSSEC на планете. Мы оцениваем, что существуют порядка, вероятно, 100 миллионов преобразователей на планете, из которых только небольшой процент фактически выполняет проверку DNSSEC. Но мы все еще говорим о порядке миллионов преобразователей, которые имеют эту конфигурационную информацию внутри. Обновление ключа - извините, ключ используется в DNSSEC для построения цепочки доверия от корня DNS до самого - конечного узла, листа дерева, которое фактически просматривается, и это обеспечивает, что данные DNSSEC, подписанные владельцем зоны, не будут - не могут

быть изменены в активном состоянии, чтобы допускать такие вещи, как атаки " человек посередине" и фишинг и тому подобное. Следующий слайд, пожалуйста.

Так почему мы обновляем ключ? Наилучшая общая практика безопасности заключается в том, что если у вас есть пароль, вы должны менять его время от времени, чтобы предотвратить ситуации, когда ваш пароль был взломан без вашего ведома, и чтобы инфраструктура, необходимая для изменения пароля, фактически работала в случае, когда вы вынуждены менять пароль по какой-то необъяснимой причине.

То же самое можно сказать и о DNSSEC. Вы можете подумать о подписании ключа как о пароле для DNSSEC, и в результате нам нужно убедиться, что инфраструктура, которая существует для изменения ключа, действительно работает, если мы когда-либо окажемся в положении, в котором нам нужно изменить ключ. Нам, например, потенциально необходимо изменить ключ, если есть какая-то прорывная технология, которая позволяет факторизовать криптографическую информацию, вы знаете, или у нас есть указание на то, что ключ был каким-то образом скомпрометирован. Проблема в том, что, учитывая количество устройств, которые мы собираемся обновить, мы должны делать это очень осторожно, очень медленно. Мы - и также предпочли бы не

нарушать Интернет, пока мы это делаем. Проблема в том, что если мы допустим ошибку во время обновления ключа, это означает, что преобразователи, машины, серверы, которые конечные пользователи используют для поиска любого имени в Интернете, спонтанно перестанут работать для любой зоны, которая подписана, и поскольку корневая зона подписана, это означает, что это будет очень плохой день для любого в Интернете. Поэтому мы предпочли бы этого не делать. Поэтому мы принимаем очень осторожный и продуманный подход, с наибольшим количеством тестирования, насколько это возможно, чтобы гарантировать, что нет существенного риска для возникновения проблемы с проверкой DNSSEC по Интернету. Так что это на самом деле это процесс в два с половиной года. Следующий слайд, пожалуйста.

Вот, пожалуйста. И это некоторые из значительных дат, которые произошли для подписания ключа, или произойдут в будущем. 19 сентября размер ключа был увеличен, потому что нам фактически пришлось вставить новый ключ в DNS для его использования в последующих так называемых церемониях подписания ключа. Церемония подписания ключа - когда мы берем - мы идем в эти безопасные объекты, берем закрытый ключ и подписываем ключ подписания зоны от VeriSign, чтобы использовать для подписания корневой зоны. Мы делаем это каждый квартал. И это означает, что

для всех этих видов деятельности это в основном синхронизируется с этими ежеквартальными управлениями ключа - церемониями подписания ключа, которые мы проводим. Таким образом, последний в сентябре - в 27 - 19 сентября 2017 года, размер ключа DNS станет больше, так как мы добавляем новый ключ. 11 октября этого года мы будем использовать этот ключ в первый раз.

И это своего рода самая вероятная дата, когда что-то странное может произойти, и странное потому, что люди, которые не изменили свой ключ к 11 октября в преобразователях, они не смогут провести валидацию. Любой поиск доменного имени, который они выполнят, приведет к "host not found" «хост не найден» или ошибке 404, что-то вроде этого.

11 января мы фактически берем старый ключ и добавляем к нему флажок-признак, говорящий, что его больше нельзя использовать. 22 марта мы фактически вытаскиваем старый ключ из корневой зоны. А затем в августе 2018 года мы фактически уничтожаем этот старый ключ, чтобы быть уверенным, что все в безопасности.

Следующий слайд.

На кого это повлияет? Ну, разработчикам и дистрибьюторам программного обеспечения DNS необходимо, чтобы новый ключ был включен в их программное обеспечение и их режимы распределения. Системные интеграторы, люди,

которые берут программное обеспечение и вводят его в действие, должны убедиться, что у них есть последний ключ в системах, которые они интегрируют. Сетевые операторы обычно являются людьми, которые управляют преобразователями. И им нужно убедиться, что их системы могут поддерживать это изменение ключа.

Операторы корневого сервера должны быть осведомлены, и мы находимся в тесном контакте с ними, потому что именно они, скорее всего, столкнутся с проблемами, если люди не поменяют ключ. В общем случае преобразователь попробует несколько раз получить - что-то преобразовать, если проверка DNSSEC не удалась. Таким образом, они увидят всплеск объема трафика.

Поставщики интернет-услуг - это люди, которым почти наверняка - почти наверняка будут звонить по телефону. Если есть какие-то проблемы, если сетевые операторы не обновляют свои - ключ, то провайдерам начнут звонить.

И конечные пользователи будут иметь последствия, если оператор сети не обновит ключ, потому что внезапно они не смогут попасть ни на какой сайт в Интернете.

Следующий слайд, пожалуйста.

Поэтому, очевидно, нам нужно тщательно подготовиться. Мы просили сетевых операторов убедиться, что они активировали

проверку DNSSEC. Если они это сделали, им необходимо убедиться, что они могут обновить этот ключ. Исторически, преобразователи как-то начали работать, вам никогда не приходило в голову об этом думать, и люди вводили их в действие в файловых системах только для чтения, что было бы проблемой, если бы вы попытались изменить ключ, потому что вы не смогли бы записывать на диск.

Следующий слайд.

Итак, что нужно делать операторам преобразователей? Им нужно знать, включен ли DNSSEC. Они должны убедиться, что они понимают, как доверие оценивается по их системам. Им необходимо проверить и убедиться, что их преобразователь способен обработать изменения в ключе, проверить файлы конфигурации, убедиться, чтобы все написано в нужном месте. И если проверка DNSSEC включена или запланирована в сети, тогда у вас есть план участия в процедуре смены ключа. Например, наблюдайте за поведением 11 октября и знайте, как некоторые вещи, скорее всего, откажут в работе. Как правило, преобразователь, который не обновил свой ключ, начнет отвечать с servfail на - покажет указание сбоя сервера, в любое время, когда кто-то выдает запрос на имя, которое было защищено.

Следующий слайд, пожалуйста.

Жалко. Маленький синий квадратик - это на самом деле является изображением письма, которое мы отправили. Но, как я уже упоминал, мы отправили письмо в органы регулирования в странах и представителям GAC, в основном предлагая, чтобы они поговорили со своими сетевыми операторами, чтобы убедиться, что они знают о смене ключа. Следующий слайд.

И это в общем-то, все. Я рад ответить на любые вопросы и рад предоставить любую информацию, которая у меня есть, чтобы помочь вам в обсуждении этого вопроса с вашими сетевыми операторами. Опять же, я Дэвид Конрад (David Conrad), david.conrad@icann.org. Благодарю вас за предоставленное время для этой презентации.

ПРЕДСЕДАТЕЛЬ SCHNEIDER: Спасибо, Дэвид. Ну, я думаю, что мой первый вопрос был бы: есть ли аналоговый номер телефонной линии, который вы можете предложить в случае прекращения функционирования всего Интернета, по которому мы можем обратиться за помощью? И будет ли он работать 24/7?

У США есть вопрос или комментарий.

DAVID CONRAD: Чтобы ответить на этот вопрос, да, Глобальная служба поддержки ICANN знает об этом, и мы разместили эти номера в разных местах.

США: Спасибо. Это была очень полезная презентация. Это проблема, близкая моему сердцу, потому что я в душе нерд. Но мы получили письмо от Йорана. Спасибо большое. И честно говоря, моя первоначальная реакция заключалась в том, что нам нужно работать с нашими интернет-провайдерами. Как правительство, мы обычно полагаемся на наши резолюции - нашу резолюцию с коммерческими интернет-провайдерами.

Но с точки зрения предоставленного нам руководства, есть ли что-то, что нам нужно сделать, как правительствам, чтобы убедиться, что наши - помимо того, чтобы убедиться, что интернет-провайдеры делают то, что им нужно делать, есть ли что-то, что вы рекомендуете нам сделать, чтобы наши операции продолжались? Спасибо.

DAVID CONRAD: Да. В любой сети, будь то правительственная внутренняя сеть или сеть интернет-провайдера, в каком-то месте должен быть какой-то преобразователь. Он может быть внешним. Например, Google предоставляет свою

общедоступную службу DNS 8.8.8.8. И многие люди используют эту услугу.

Все это, вы должны убедиться, что они могут справиться со сменой ключа.

Google, безусловно, способен справиться со сменой ключа, насколько я знаю. Я не сомневаюсь - я не сомневаюсь в этом.

Но для других интернет-провайдеров, других сетевых операций, в частности сетевых операций на уровне предприятия, хорошо - просто спросить, знают ли они, что ключ изменится. И если они ... ну, они должны сначала проверить, включен ли DNSSEC, и, если возможно, настоять, чтобы DNSSEC был включен. Но тогда, если он включен, проверьте, знают ли они, что ключ изменится. И если это не так, предложите, чтобы они приняли участие в усилиях по смене ключа, которые рекламирует ICANN.

То, что мы делаем здесь, отражает то, что мы делали на многих площадках, в основном мы просто пытаемся сделать - повысить осведомленность о том, что это происходит, но очевидно, что мы не сможем связаться со всеми. Поэтому мы действительно просим, вы знаете, правительства предпринять определенные усилия, чтобы сетевые операторы знали, что произойдет смена ключа.

ПРЕДСЕДАТЕЛЬ SCHNEIDER: Иран.

ИРАН: Большое спасибо за презентацию. Есть ли у вас канал обратной связи, чтобы убедиться, что действие, которое вы указали, должным образом выполнено до того, как что-то сломается? Не все так знакомы и так быстро следуют за действиями. Так что просто вопрос обратной связи, да, мы получили ваше письмо, мы это реализуем. Возможно, указать на любую потенциальную трудность? Или у вас нет такой системы обратной связи? Спасибо.

DAVID CONRAD: Мы вообще, во всех случаях, что мы, вы знаете, говорили, мы призываем людей связаться с нами, задавать любые вопросы, которые у них могут быть, или любые беспокойства, которые они могут пожелать выразить.

У нас нет явного механизма для того, чтобы требовать от людей обратной связи. Но мы работаем, в частности, с различными группами сетевых операций, различными организациями TLD, такого рода вещи, чтобы обеспечить место, в котором, вы знаете, могли бы быть созданы каналы связи, позволяющие нам получать такую обратную связь.

ПРЕДСЕДАТЕЛЬ SCHNEIDER: Спасибо. У меня есть Египет, Норвегия и Великобритания. Нидерланды, извините.

ЕГИПЕТ: Спасибо, Томас. И спасибо, Дэвид, за презентацию. У меня вопрос по слайду 5. Но между тем, если я правильно понимаю, есть какой-то инструмент, чтобы проверить, что вы готовы - я думаю, это полезно знать.

DAVID CONRAD: Да. Мы создали испытательную платформу, которая позволит операторам преобразователей участвовать в тестировании процедуры обновления KSK в режиме реального времени. К сожалению, испытательная платформа не в этом наборе слайдов. Она была более ориентирована на более технический набор слайдов, но я могу предоставить эту информацию членам GAC для предоставления своим сетевым операторам в своих странах.

ЕГИПЕТ: Спасибо. Я думаю, что это очень полезно.

И мой вопрос по слайду 5, пожалуйста.

Просто чтобы убедиться, влияет ли это на преобразователей конкретно? Потому что я не вижу здесь ccTLD - я имею в виду

регистратур TLD, операторов. Так это преобразователи конкретно? Спасибо.

DAVID CONRAD: Верно. Итак, люди, которые затронуты здесь, находятся на стороне DNS, которая фактически извлекает информацию от операторов TLD. На TLD, ccTLD, gTLD не будет оказано влияние при смене ключа.Им не нужно ничего делать. Разумеется, нет никакой функциональности, которую они предоставляют, на которую будет оказано влияние, кроме их внутренних систем и преобразователей, с которыми они работают в своих внутренних системах.

ПРЕДСЕДАТЕЛЬ SCHNEIDER: Спасибо. Нидерланды.

НИДЕРЛАНДЫ: Да, спасибо, Дэвид, за ваше объяснение. Просто дважды проверю пару вещей. Я думаю, что у правительств нет официальной ответственности в этом. Но вы используете их просто как каналы, чтобы связаться с интернет-провайдерами. Но нет, допустим, правительственной ответственности?

DAVID CONRAD: Точно. Мы ищем любой канал связи, который мы можем использовать, да.

НИДЕРЛАНДЫ: Во-вторых, был список DNS-преобразователей, рекурсивных преобразователей, которые выполняют проверку DNSSEC в каждом письме. В нашем случае, я думаю, сейчас около семи или восьми. Конечно, с ними напрямую связались, я полагаю, и это именно те, кто действительно должен сделать изменения, реальные изменения в своих системах. Другие затронутые заинтересованные стороны действительно имеют последствия, но действительно ли им приходится менять свои системы? Спасибо.

DAVID CONRAD: Итак, реальная операция того, как произойдет изменение ключа, на самом деле существует автоматический режим, если вы работаете в актуальном состоянии - если оператор преобразователя работает с обновленным программным обеспечением и включили автоматические обновления, тогда им фактически ничего не нужно делать. Вероятно, было бы разумно участвовать в испытательной платформе, чтобы гарантировать, что ничего странного не произойдет, когда фактически произойдет смена ключа. Но, в конечном итоге, в современных преобразователях встроена автоматизация, которая автоматически будет обрабатывать эту смену ключа.

Если они не работают со старым - извините, не работают с новым программным обеспечением или они не включили автоматическое обновление, тогда им нужно изменить точку данных конфигурации. Это фактический - открытый ключ, связанный с KSK, его нужно будет скопировать в файл конфигурации. Так вот в том случае, когда операторы преобразователя должны будут предпринять какие-то действия.

ПРЕДСЕДАТЕЛЬ SCHNEIDER: Спасибо. Великобритания кратко.

ВЕЛИКОБРИТАНИЯ: Да, спасибо. Спасибо, Дэвид, за ваш брифинг по этой теме.

Я на самом деле не разговаривал с членами британского сообщества провайдеров, ISPCP. В принципе, это все материалы для подключения, поэтому я проверю. Но я полагаю, вы бы хотели, чтобы они провели информационно-разъяснительную работу, для интернет-провайдеров по всему миру. И уверены ли вы, что это происходит? Было бы очень полезно получить это заверение.

И на самом деле я не видел письма, поэтому я должен и это проверить. Я не знаю, где это могло оказаться.

Но я думаю, что я также слышал, как вы говорите, что для нас будет ценным двойная проверка с нашей глобальной сетью - правительственными сетевыми провайдерами. Для меня это офис в Лондоне. Что вы делаете 11 октября? Вы с нетерпением ждёте того дня? Я имею в виду, если есть что-то, что может пойти не так, потому что люди не провели необходимое переключение, если это правильное слово, будет ли какое-то возвращение к нам, как правительствам, для защиты всего? Или как вы справитесь со значительным провалом в тот момент 11 октября? Да извините.

DAVID CONRAD: Да, мы были в контакте с ISPCP и призвали их связаться со своими членами и другими органами, с которыми мы имеем дело, вы знаете, активно участвуя в заседаниях групп сетевых операторов.

«Что касается- если случится что-то плохое, мы - мы создали очень сложную систему наблюдения, чтобы наблюдать за трафиком на корневые серверы, что было бы одним из первых признаков того, что что-то не так. И у нас есть резервные планы, которые будут реализованы, если - мы обнаружим, что вы знаете, какое-то значительное событие, указывающее на то, что смена ключа завершилась неудачей.

Мы достаточно уверены в том, что маловероятно, что правительства, вероятно, получат гнев от конечных

пользователей и сетевых операторов. Я ожидаю, что это будет фактически нацелено на ICANN или, более конкретно, на меня, и это одна из причин, по которой я очень старался распространить информацию по этому поводу, что очень важно, чтобы люди обновили свой ключ.

ПРЕДСЕДАТЕЛЬ SCHNEIDER: Простите. Пожалуйста, не выходите из зала. Есть важное объявление, которое я собираюсь сделать через одну минуту, поэтому позвольте мне просто дать слово джентльмену сзади. Я думаю, что если я - это Нигерия, верно?

НИГЕРИЯ: Нигерия, да.

ПРЕДСЕДАТЕЛЬ SCHNEIDER: Спасибо. И, пожалуйста, не выходите из зала. Это последнее выступление, которое мы позволим, и затем нам придется завершить. Более или менее строго. Нигерия, пожалуйста, продолжайте.

НИГЕРИЯ: Спасибо за презентацию об обновлении ключа DNSSEC.

Мой вопрос в том, что для тех поставщиков сетевых услуг, которые не включили DNSSEC, что происходит с ними после

смены ключа? Те, которые изначально не включили DNSSEC в свои сети. Спасибо.

DAVID CONRAD: Да. Они не заметят никаких изменений. Если они не включили DNSSEC, смена ключа никак не повлияет. Если в какой-то момент в будущем они решат включить DNSSEC, им необходимо убедиться, что у них самый последний ключ. Если они этого не сделают, то их проверка не удастся, и это произойдет - там возникнет путаница. Поэтому им просто нужно убедиться, что у них самый последний ключ или самое последнее программное обеспечение, который, скорее всего, автоматически получит последний ключ.

ПРЕДСЕДАТЕЛЬ SCHNEIDER: Мы должны на этом завершить заседание, потому что есть несколько желающих кратко выступить, а затем мы знаем, что из этого получится, потому что у нас есть важное для вас сообщение. Это, как вы знаете, это наш последний обед на этой встрече или в обеденное время, и это означает, что это последнее обеденное время для Олофа в его функции -

Какова ваша функция, на самом деле? Сотрудник ICANN, который поддерживают GAC и отпускает хорошие шутки в любое время дня и ночи на телеконференциях и тому подобное, например, когда необходима поддержка.

Так вот, Джулия, которая, вероятно, снова где-то прячется, на самом деле организовала, помогла нам организовать небольшой подарок для Олофа.

[Смех]

Вы увидите - мы проверим с техническими работниками, как это поставить. Это справедливо - я думаю, там есть карточка, и это и есть подарок. Он не слишком тяжелый, поэтому он должен действительно работать, поэтому мы просто хотим снова и снова, и действительно, и на самом деле и со всей нашей радостью сказать спасибо вам, Олоф.

И есть там в задней части зала есть бокалы, некоторые напитки и некоторые закуски, чтобы отпраздновать последние моменты с Олофом в этой функции. Большое спасибо, Олоф.

[Аплодисменты]

OLOF NORDLING: Спасибо огромное. Я всегда хотел наковальню -

[Смех]

- как удобный ручной багаж.

О, это здорово. Огромное спасибо. И, надеюсь, я останусь на связи, хотя я пойду на пенсию и так далее.

Так что - и я все равно буду до конца июля, так что - ну, вы еще не избавитесь от меня, но спасибо вам большое.

ПРЕДСЕДАТЕЛЬ SCHNEIDER: Хорошо. Мы все можем вернуться к –

БРАЗИЛИЯ: Томас, позвольте Вас спросить?

ПРЕДСЕДАТЕЛЬ SCHNEIDER: Да.

БРАЗИЛИЯ: Что касается после обеда, мы собираемся встретиться здесь, и затем у нас есть гео названия, но что мы намерены делать? Потому что я думаю, что нам также нужно в какой-то момент собраться вместе, чтобы обсудить коммюнике, или это не понадобится?Что будет в этом отношении? Потому что вчера мы говорили о встрече где-то в 15:00 или провести какое-то взаимодействие.

ПРЕДСЕДАТЕЛЬ SCHNEIDER: Мы будем - мы рассмотрим куски текста, которые у нас уже есть - или мы уже получили.У Тома есть общий обзор. Мы посмотрим на это во время обеда в какой-то момент времени, а затем после - идея состоит в том, чтобы к 15:00 все было

готово, а затем, может быть, потратить пять минут или около того, надеюсь, на завершение этого. Но спасибо, что напомнили нам.

Так что не убегайте. Работа еще не закончена. Спасибо.

Но во-первых, это не работа, это празднование Олофа. Спасибо.

[Перерыв]