ICANN73| Неделя подготовки — Отчет о работе Программы по обмену знаниями и запуску стандартов для DNS и безопасности в области присвоения имен (KINDNS)
Среда, 23 февраля 2022 года, 11:00 – 12:00 по AST

АДИЭЛЬ АКПЛОГАН: Мы кратко расскажем вам о программе KNDNS, которая является инициативой по продвижению передовой практики DNS в целом. Сегодня у нас есть перевод, поэтому мы просим вас воспользоваться переводом. Докладчик будет стараться по возможности говорить медленно и внятно, чтобы переводчик мог выполнить свою работу.

Задавайте свои вопросы функции вебинара Q&A, чтобы их можно было передать нам. Если захотите высказаться, вы можете поднять руку, и вам дадут слово. Стивен, следующий слайд, пожалуйста.

Итак, мы проведем эту презентацию в двух частях. Я сделаю первое вступление, а затем представлю вам [Филипа Рено], нашего эксперта по этому проекту, который выскажется по существу этого проекта и пояснит, на каком этапе мы находимся.

Итак, во время ICANN72 мы провели заседание, на которой представили KINDNS и немного объяснили, что мы хотим сделать, поэтому я начну прямо с того, что такое KINDNS. Это ассоциация по обмену знаниями, имеющая дело с безопасностью DNS и [именования]. Короче говоря, речь идет об обмене передовым опытом и о возможности работать с сообществом и оператором

DNS в целом, чтобы добровольно добавить свои комментарии к этому передовому опыту, а также помочь всем нам в ICANN продвигать передовой опыт во всем мире и убедиться, что мы, как обычно, работаем вместе, делая систему DNS как можно более безопасной. Следующий слайд, пожалуйста.

Некоторые из вас уже знакомы с MANRS, которая представляет собой инициативу по обеспечению безопасности маршрутизации в Интернете. KINDNS играет в этом небольшую роль, так что мы можем сказать, что если у нас есть хорошие MANRS и KINDNS, мы сделаем немного больше для обеспечения безопасности и сохранения Интернета для всех.

Мы хотим создать оптимальную передовую практику, которой можно легко следовать для обеспечения безопасности работы DNS, и мы хотим сделать акцент на работе DNS, потому что это будет чисто техническая передовая практика по работе DNS. Обычно вокруг DNS работают все службы, приложения, и эта инициатива попытается сосредоточиться конкретно на работе DNS, на техническом аспекте этой работы.

Если вы знакомы с DNS, то, вероятно, слышали о DNS [неразборчиво], в котором определены все лучшие практики [неразборчиво], связанные с DNS, а это очень много, более 2000 страниц, рассказывающих о DNS. Мы пытаемся выяснить, что является наиболее важным из всего этого, что должен делать

любой оператор, управляющий любым компонентом DNS, чтобы обеспечить безопасность DNS. Следующий слайд, пожалуйста.

Таким образом, инициатива была разделена на несколько компонентов. Первый — определить и задокументировать наиболее важные нормы безопасности для операций DNS. Это делается с помощью Фила Рено, о котором я упоминал ранее, и в некоторой степени с помощью сообщества, потому что у нас есть лист рассылки, где мы регулярно делимся тем, что появляется в результате этой работы по уведомлению о норме и получению отзывов от сообщества.

Затем, основываясь на этих передовых практиках, мы запустим специальный портал для публикации передовых практик, где будем публиковать рекомендации по их внедрению, а также предоставим сообществу место, где можно оценить обычную или полезную информацию, где операторы, которые поддерживают инициативу и привержены внедрению этих передовых практик, также смогут присоединиться и помочь нам продвигать передовые практики, как я уже говорил ранее.

Итак, все будет [неразборчиво] опубликовано на специальном сайте с доменным именем KINDNS.org. Как только мы это сделаем, мы снова начнем работать со всеми, чтобы определить ряд показателей, которые помогут нам увидеть влияние инициативы на безопасность DNS, определить некоторые ключевые показатели, которые мы сможем измерить с течением времени и

посмотреть, как они развиваются в правильном или неправильном направлении, и внести соответствующие коррективы. Это будет следующий этап после того, как мы запустим этот.

Обычно, когда мы представляем это в контексте ICANN, создается впечатление: затронет ли это функцию обеспечения DNS? Имеются в виду также передовые практики регистратур, регистраторов и владельцев доменов.

Короткий ответ — в начале нет, потому что, как я уже говорил, это направлено и нацелено на основную функцию DNS. Но, возможно, на другом этапе мы рассмотрим, как можно перенести некоторые из этих передовых практик на систему обеспечения, то есть на передовые практики регистратур и регистраторов, и добавим это в инициативу. Но это уже [неразборчиво], но на первом этапе основное внимание будет уделено эксплуатации. Следующий слайд, пожалуйста.

Мы сосредоточились на определенных категориях. Опять же, если вы используете DNS, вы используете ее в среде, и есть другие компоненты, которые способствуют надежности и безопасной работе DNS в целом.

Как я уже говорил, мы не собираемся исправлять все, а сосредоточимся практически на компонентах DNS, то есть на авторитативном сервере, работающем в различных средах, то есть на TLD или люди, которые управляют критически важной зоной,

могут быть вторым уровнем. И менеджер доменных имен второго уровня в целом. Итак, у нас есть TLD в критически важной зоне, например [.seal.uk] или любой NIC.TLD являются критически важными для работы этих TLD, поэтому мы добавим их в эту первую категорию. И вторая категория — это все, у кого есть любой регистратор, управляющий доменным именем второго уровня.

Тогда мы имеем оператора резолвера рекурсивного сервера в общем случае. В этой категории также есть три подкатегории, которые мы будем рассматривать: частный (закрытый) резолвер, общий частный резолвер и публичный резолвер.

Поэтому передовые практики, которые мы будем продвигать, будут связаны с этими пятью категориями. Кроме того, мы предоставим руководство о том, как [неразборчиво] операционную среду с точки зрения обслуживания, системы и сети, а также затронем некоторые соображения конфиденциальности, которые влияют на некоторые аспекты безопасности в целом.

На этом этапе, если какие-либо операторы захотят присоединиться к KINDNS и работать с этой инициативой, они будут оцениваться снова — или самооцениваться снова — только по двум основным категориям, которые я упомянул, и которые будут определены либо в работе авторитативного сервера, либо в работе резолвера в целом.

Мы, конечно, опубликуем руководство по внедрению, как это сделать, контрольный список, процесс настройки, примеры и т. д. Возникает вопрос, к какому программному обеспечению мы будем предоставлять руководства. Мы рассмотрим самое популярное из них, но, конечно, если мы представим его так, чтобы люди поняли концепцию, они смогут легко применить эти понятия к любому другому действующему программному обеспечению. Следующий слайд, пожалуйста.

Далее я предоставлю слово Филипу, чтобы он рассказал о различных элементах, которые мы рассматривали в этих категориях. Филип?

ФИЛИП РЕНО (PHILIP REGNAULD): Да. Спасибо за вступление, Адиэль. Это очень интересный проект, и я надеюсь, что мы сможем получить от сообщества отзывы о различных передовых практиках, которые мы определили и предлагаем.

Разделив и классифицировав типы операторов DNS, мы решили заняться... Изначально мы думали, что может быть что-то вроде доменов верхнего уровня и доменных имен второго уровня. Оказалось, что все было не так просто, немного сложнее.

Поэтому мы решили сначала определить, кто будет оператором авторитативных доменных имен или оператором DNS-серверов, предлагающих услуги рекурсивного резолвера.

Итак, начав с авторитативного сервера, мы рассмотрели типы зон в Интернете по иерархической природе. Важность DNS, конечно, возрастает по мере того, как вы поднимаетесь – очевидно, что корневой сервер является наиболее критичным и, возможно, наиболее – не уязвимым, извините, но наиболее востребованной целью, если вы собираетесь скомпрометировать его, если вы собираетесь создать инцидент в области безопасности, это будет первоочередной выбор.

Таким образом, TLD занимают важное место. Но мы также рассмотрели и другие домены, которые могут иметь важное значение. Например, если мы посмотрим на DNS-серверы многих стран, то нередко можно увидеть, что, например, в Дании (DK), где я сейчас живу, DNS-серверы домена DK размещены в субдомене nic.dk. Возможно, эти домены второго уровня будут не менее важны, чем TLD, в которых размещены их DNS-серверы.

Поэтому мы решили разделить эти категории следующим образом. Мы называем их критически важными зонами. Очевидно, домены верхнего уровня и все вспомогательные или так называемые зоны поддержки, которые используются для предоставления услуг того или иного рода, либо размещения DNS-серверов или подобных взаимозависимых элементов.

И еще одно, что мы решили включить в критически важные зоны, не связано напрямую с работой самой DNS, но если посмотреть на это с точки зрения ccTLD, некоторые файлы корневых зон или

имена DNS, которые связаны с очень важными системами, будь то здравоохранение, электронное правительство, системы идентификации гражданских услуг, есть такие, которые, возможно, более важны, чем другие, но в данном случае я привел пример. В Дании существует национальная система идентификации, и я понимаю, что если сайт myid.dk не работает, многие люди не смогут войти в систему. И вы можете подумать, как это повлияет на DNS, это будет определяться моделью самооценки, и что мы действительно хотим сделать здесь, так это не обязательно диктовать, какие зоны являются критически важными, а какие нет. Это скорее основа для того, чтобы люди могли определить: использую ли я критически важные зоны? Или чтобы организации могли определить: предоставляем ли мы критически важные услуги? Поэтому, каковы рекомендации? Какой передовой практике мы должны следовать для защиты этих услуг?

Разумеется, мы также включили такие сайты, как финансовые и банковские, которые можно считать критически важными для функционирования экономики и страны.

Я бы не назвал это произвольным решением, но мы хотели структурировать это таким образом. Кроме того, с точки зрения уязвимости и воздействия на избирателей, экономику, страну, что произойдет, если эти доменные имена выйдут из строя, причем наиболее критичным будет сам ccTLD? Следующий слайд, пожалуйста.

И есть другие доменные имена. Это, конечно, все остальные доменные имена, расположенные ниже доменов верхнего уровня. Они также важны. Они будут предоставлять все различные услуги и веб-сайты, электронное управление, электронную коммерцию и все то, что, как мы знаем, есть в Интернете. Ими тоже нужно управлять ответственно.

То есть, это не потому, что они второсортные граждане или что-то в этом роде, но, возможно, будет несколько меньше ограничений в отношении передового опыта, который мы хотим использовать, и причина в том, что мы хотим провести эту операцию, возможно, для того, чтобы поощрить людей прийти, чтобы начать работать с KINDNS, начать применять этот передовой опыт и не быть отпугнутыми сложностью, и поэтому, если вы управляете доменом второго уровня, вы, вероятно, не так сильно повлияете на других людей, поскольку вы не управляете делегированием, но у вас все еще есть... Вы можете подвергнуться кибератаке. Вы можете быть подвержены системным сбоям. А вы проводите комплексные проверки? Используете ли вы передовые практики, которые позволят вам либо смягчить последствия этих инцидентов, либо хотя бы восстановиться после них?

И не имеет значения, насколько важен домен в этом отношении. Все должны это делать, потому что неправильно настроенный или захваченный домен так или иначе приведет к сбоям в работе. Следующий слайд рассказывает... Да.

Итак, операторы рекурсивных DNS. Это вторая половина экосистемы, правильно? У нас есть авторитативные операторы и рекурсивные операторы DNS, и здесь нам нужно было рассмотреть, какие рекурсивные резолверы у нас есть.

В двух словах, они будут либо публичными, либо частными. Если присмотреться внимательнее, то будут частные резолверы, и это будут полностью корпоративные сети, полностью закрытые, недоступные извне, доступ типа VPN и обычно в частном адресном пространстве, и это будут компании и организации, такие как здравоохранение и банки, и большинство предприятий будут структурированы подобным образом. Но в некоторой степени это также домашние сети и, возможно, городские сети.

И есть немного более открытые общие частные резолверы, и это, возможно, забавное имя, но мы пытаемся найти что-то, что... Я не хотел указывать необходимых провайдеров или любого рода провайдеров. Мы говорим «общие частные», потому что они являются частными для ряда клиентов или, возможно, ряда учреждений. Мне представляется университетская сеть. Они недоступны извне, но все равно используются совместно, возможно, юридически разными организациями. Например, несколько клиентов совместно используют резолвер интернет-провайдера, или это может быть в контексте объединенного набора организаций под единым техническим управлением.

Это будет еще одна категория, а после нее у нас будут публичные резолверы. Публичные резолверы хорошо всем известны. На память приходят 8888 от Google или Quad9 и подобные службы, но между ними и фактически закрытой службой DNS есть коммерческая фильтрация DNS, которая может быть или не быть открытой в той или иной форме, но... Извините, я постараюсь говорить немного медленнее.

Для публичных резолверов у нас есть, как мы уже говорили, Google и подобные, а также полуоткрытые или — как там они называются? Открытые резолверы с коммерческим компонентом, где при правильном соглашении или контракте вы получите дополнительные услуги от этих конкретных операторов резолверов в виде очистки или пассивного DNS-сервиса, где ваш DNS-трафик анализируется, чтобы выяснить, есть ли у вас узлы, которые скомпрометированы или заражены вредоносным ПО.

И эти типы операторов обычно являются общедоступными, но у них есть какой-то механизм контроля доступа и, возможно, какая-то плата, которую нужно внести или заключить контракт, чтобы вы могли пользоваться их услугами и получать выгоду от дополнительных — как там они называются? Дополнительных услуг, которые они будут предоставлять.

Итак, это различные категории, и в разделе выше мы определяем, как эти резолверы — как ограничивается доступ к этим резолверам? Это будет сочетание доступа по IP-адресу, или это

могут быть сертификаты, или это может быть VPN. На самом деле это не имеет значения. Что действительно важно здесь, так это то, что мы пытаемся отнести каждого из этих операторов к определенной категории, где они могут пойти и посмотреть на KINDNS и сказать: «Ну, хорошо, это относится к нам. А каковы передовые практики?».

А также, в некоторой степени, возможно, для конечных пользователей и организаций. Например, предприятие, которое захочет посмотреть: «Эй, я подключаюсь к своему интернет-провайдеру. Я использую его резолвер для передачи своих запросов к DNS в интернет.». Какую передовую практику они должны использовать и придерживаются ли они ее? Действительно ли они следуют программе?

Затем вы можете обратиться к своему провайдеру, интернет-провайдеру или в свой ИТ-отдел. Следуем ли мы KINDNS в этих передовых практиках работы с резолверами? Защищаем ли мы конфиденциальность наших пользователей так, как это описано здесь? Следующий слайд.

Итак, рекомендации для частных резолверов. Мы не рассмотрели многие рекомендации для авторитативных резолверов, но сейчас это не столь важно. Сосредоточим внимание на частных.

Частные резолверы, как мы уже говорили, находятся в частных сетях. В некоторых случаях они являются частью доверенного

конкурирующего домена, например, Active Directory и т. п. Вы найдете их во многих средах Windows.

Вот что мы сделали, когда сосредоточились на них: мы сосредоточились в первую очередь на безопасности сети и определили также необходимость транспарентности. Это означает, что определенные рекомендации, которые могут иметь смысл в других местах, например DoH или DoT, многие из этих сетей все еще не уверены в возможности использования этих услуг, но они все еще могут извлечь выгоду из использования DoH или DoT, и пересылки своих запросов на вышестоящий резолвер, который имеет безопасность — простите, шифрование, позволяющее вам, по крайней мере, защититься от прослушивания запросов на пути из сети. Таким образом, для каждого из операторов это немного разный сценарий.

Затем, доступность и отказоустойчивость услуг. Как упомянул Адиэль, некоторые из этих передовых практик будут включать старые добрые передовые практики системного администрирования, и поэтому мы не будем углубляться в них сейчас, но они будут подробно описаны на сайте и в программе, чтобы по крайней мере было на что ссылаться в плане укрепления системы и надлежащего системного администрирования.

И на первом месте здесь мы видим проверку DNSSEC. Я забыл об этом упомянуть. Для авторитативных серверов мы, конечно, ожидаем, что одной из ведущих передовых практик, которую мы

будем продвигать для операторов авторитетных зон, будет подписание DNSSEC, и здесь, на стороне резолверов, мы будем поощрять — или, скорее, делать это требованием — для резолверов проводить проверку DNSSEC.

К счастью, это уже сделано для многих существующих программ, но мы сделаем это, подчеркнем это и скажем, что вы должны выполнять проверку DNSSEC в данный момент времени. Опять же, вероятно, это уже распространяется на многие программы. Следующий слайд.

Итак, общие частные резолверы, о которых мы говорили, относятся к типам интернет-провайдеров. Это интернет-провайдеры или аналогичные организации. У них будут такие же требования, как и у многих частных резолверов, но у них будет другой спектр клиентов, потому что они будут иметь дело, возможно, с комбинацией мобильных, кабельных, оптоволоконных и жилых сетей. Должен быть определенный контроль доступа.

А поскольку эти резолверы используются совместно многими различными клиентами, возникает проблема конфиденциальности. Существуют такие вещи, как перехват кэша и другие вещи, о которых мы сейчас не будем говорить. Но вы хотите быть уверены, что, предлагая услуги DNS, вы делаете это с соблюдением конфиденциальности, и поэтому мы рекомендуем включить DoH или DoT или и то, и другое в вашей службе

резолвера, чтобы ваши клиенты, которым удобнее пересылать запросы вам, могли это делать. А также не поддаваться соблазну, а чувствовать, что они могут воспользоваться вашими услугами и им не придется искать решение в другом месте из-за задержки. Они могут использовать вашу сеть, предлагая DoH и DoT. Они могут использовать ваши системы и знают, что у них уже есть деловые отношения с вами как с интернет-провайдером. Тогда вам следует предложить DoH и DoT. Это просто логично с точки зрения конфиденциальности. И это, конечно, наряду с существующим традиционной и шифруемой DNS, которая будет существовать еще долгое время.

Доступность и отказоустойчивость службы DNS. Там есть ряд рекомендаций, которые мы также даем. Они будут размещены в Wiki и на сайте в ближайшее время, и это опять же хорошая системная практика, гигиена, укрепление. И снова — проверка DNSSEC. На данный момент можно было бы ожидать, что любой пользователь, работающий с резолвером ISP, будет выполнять проверку DNSSEC. Следующий слайд.

Что касается операторов публичных резолверов, мы говорим в основном о крупных открытых операторах, таких как Google и все остальные. Конечно, у них есть свои методы работы, но я уверен, что многие из них уже применяют многие из этих передовых практик, и одна из вещей, которые мы вводим [неразборчиво] сейчас — это проверка DNSSEC, и, к счастью, крупные компании занимаются проверкой DNSSEC и конфиденциальности, DoT, DoH.

Все крупные компании предлагают либо DoT, либо DoH, либо и то, и другое, поэтому можно направлять запросы, например, в Quad9 или Cloudflare по номеру 1111 и использовать их услуги DoT или DoH.

Еще одна вещь, о которой мы упомянули — QName Minimization, и забыли упомянуть об этом для других, но QName Minimization позволяет избежать ненужной утечки полностью определенных имен доменов в сторону корня. Включив эту функцию, вы раскрываете только часть доменного имени, потому что, хотим мы того или нет, доменные имена раскрываются. Они раскрывают информацию о наших пользователях, их привычках и о том, что они просматривают. Это не всегда предназначено для общественного потребления.

То же самое касается и закрытых публичных резолверов, предлагающих услуги либо за плату, либо на основе какого-то соглашения или контроля доступа, им также придется предлагать DoT/DoH, что, вероятно, уже имеет место для многих из них.

И QName Minimization почти всегда включена в настоящее время как стандартная практика, но теперь мы делаем это, так сказать, требованием. И проверка DNSSEC, конечно. Следующий слайд.

Этом, наверное, все, что я хотел рассказать.

АДИЭЛЬ АКПЛОГАН: Дальше я сам. Спасибо. Итак, эта часть от Фила дает вам общее представление о том, как будут структурированы различные передовые практики. Опять же, имейте в виду, что наша цель здесь — упорядочить это и сосредоточиться на самом важном, оставив только определенное количество передовых практик для внедрения, не больше, чем наша цель — 7:10 практик в целом для людей, чтобы они могли подобрать их для себя, чтобы не запутать их еще больше.

Далее я хочу дать вам небольшой обзор того, как все это будет представлено и структурировано, когда мы это запустим. Как я уже говорил, он будет размещен на сайте KINDNS.org, специальным сайте для этого. Он поддерживается и спонсируется в первую очередь ICANN, где люди, заинтересованные в том, чтобы присоединиться к инициативе различными способами, смогут получить необходимую им информацию.

Поэтому будет проведена сессия, затрагивающая различные категории, о которых говорил Фил. Зона поддержки и участия предназначена для операторов, желающих присоединиться к инициативе и поддержать ее, здесь они смогут зарегистрироваться в качестве спонсора, участника, оператора домена или посла инициативы.

Затем мы проведем заседание по инструментам, где операторы смогут провести самооценку. Мы все еще обсуждаем и рассматриваем, каким будет инструмент самооценки. Мы хотим,

чтобы это было очень легко, просто, понятно, потому что мы не делаем это обязательным. Это добровольное участие, поэтому люди должны взять на себя обязательства по внедрению этих передовых практик в целом.

Таким образом, инструмент самооценки также будет основан в основном на самообязательстве людей внедрить некоторые из этих практик и ответить на эти вопросы заранее.

У нас будет панель управления. Мы разработаем панель управления, которая даст нам некоторую информацию. И, как я уже упоминал ранее, возможность отслеживать некоторые идентификаторы, которые мы выбрали, чтобы мы могли видеть, как это влияет на картину в целом. А затем у нас также будет руководство по внедрению передовых практик или предоставление более подробной информации о любой из передовых практик или соображений.

Например, если вы посмотрите на слайд, на котором Филип упомянул все, что связано с укреплением ядра или безопасности системы, и все эти вещи, которые не будут частью основных передовых практик, будут выделены, например, в руководствах, где люди смогут ознакомиться с ними. Но они не относятся к сути того, что мы хотим делать. Затем у нас будет блог, мероприятия и все остальное, связанное с этим.

Поэтому, работая над этим, обобщая и выявляя наиболее важные передовые практики, мы также приступили к разработке

некоторых рекомендаций. Недавно мы выпустили руководство по подписи DNSSEC в одном из наших документов [OCTO]. Ссылки на эти документы будут даны в KINDNS, и в ближайшее время будет выпущено еще много рекомендаций. Следующий слайд, пожалуйста.

Сейчас у нас есть подрядчик, который поможет нам в проектировании и разработке нового веб-сайта. Он, вероятно, будет выглядеть примерно так, но мы находимся на очень ранней стадии [помощи] им в определении окончательного макета и окончательного дизайна этого сайта. Но на самом деле это будет самым ближайшим результатом для этого проекта в целом. Следующий слайд.

Итак, по разным причинам нам пришлось немного скорректировать наши сроки с момента последней презентации, но сейчас наша цель — запустить эту программу к концу первого квартала 2022 года, то есть примерно к концу марта.

Возможно, у нас не будет всех функций сайта, но мы запустим самую важную, которая позволит нам начать работать с этим, начать разворачивать и наблюдать за ситуацией с операторами.

Мы будем информировать сообщество и обновлять лист рассылки по мере продвижения. Если вас это заинтересовало, я рекомендую вам присоединиться к листу рассылки. Лист рассылки открытый. Любой желающий может присоединиться и предоставить нам обратную связь и внести свой вклад в обсуждение этого вопроса.

А пока в качестве временного хранилища мы создали страницу Wiki, где мы публикуем большинство вещей, над которыми мы сейчас работаем. Они будут перенесены на официальный сайт, когда мы [добавим их].

По-моему, это последний слайд. Да. Большое спасибо всем за внимание. Мы хотели бы услышать от вас любые вопросы, комментарии, предложения. Вот для чего нужна эта сессия. Спасибо.

КИНГА КОВАЛЬЧИК (KINGA KOWALCZYK): В модуле Q&A есть вопрос. Адиэль, хотите, чтобы я зачитала его?

АДИЭЛЬ АКПЛОГАН: Да, пожалуйста.

КИНГА КОВАЛЬЧИК: У нас вопрос от участника по имени Шивасубраманьян (Sivasubramanian). «Может ли KINDNS также выработать общее обязательство не привязывать пользователей к одному резолверу, а поддерживать несколько резервных резольверов, которые может использовать каждый? [Грубый], неточный, несколько надуманный сценарий. Этот [неразборчиво] университет запрещает студентам использовать внешние резолверы или мэр настаивает на том, чтобы каждый житель

города не использовал другой городской резолвер? Это и другие соответствующие совместные обязательства, помимо обмена передовым опытом».

АДИЭЛЬ АКПЛОГАН: Спасибо. Очень интересный сценарий. Вопросы уместны и относятся к владельцам доменов, к пользовательской части этого собрания. И большинство из них связаны с политикой, потому что это политические решения, когда кто-то просит своего клиента, своего пользователя, свое сообщество, своего жителя использовать определенного оператора или определенную услугу. И политические аспекты не рассматриваются здесь каким-либо образом, потому что у нас очень мало контроля над такими вещами.

С точки зрения регистратора и выполнения операций, конечно, вы можете установить несколько резолверов в вашей системе, и это общая передовая практика для управления сетью, общая передовая практика для предоставления услуг или для отказоустойчивости и избыточности службы DNS в целом. Но мы не уделяли этому аспекту особого внимания, потому что это больше относится к передовым практикам владельцев доменов и интернет-провайдеров, а не к сути работы DNS, как таковой.

КИНГА КОВАЛЬЧИК (KINGA KOWALCZYK): Больше вопросов нет. Пожалуйста, если вы хотите задать вопрос, поднимите руку, и мы включим ваш микрофон и предоставим вам слово, или введите свой вопрос в блок Q&A, и я зачитаю его вслух.

АДИЭЛЬ АКПЛОГАН: Я хотел бы услышать мнение участников об одном из аспектов этого. Фил упомянул об этом. Я думаю, что это было на слайде, посвященном публичному резолверу, где мы подчеркиваем соображения конфиденциальности. Этот аспект мы много обсуждали между собой.

Как вы все знаете, DoH и DoT вначале были очень противоречивыми, вызывали некоторые опасения, но все больше и больше операторов резолверов внедряют это, и это хорошая практика для конфиденциальности в целом.

Вопрос в том, насколько эти соображения конфиденциальности должны быть частью KINDNS? Если посмотреть на обычную документацию по передовым практикам, то до прошлого года большинство из них... Соображениям конфиденциальности уделялось недостаточно внимания. Но за последние несколько лет конфиденциальность стала очень важным фактором для пользователей в Интернете.

Поэтому мы посчитали, что конфиденциальность должна быть учтена в KINDNS в целом. QName Minimization распространена

повсеместно, как с точки зрения резолверов, так и с точки зрения их работы, это просто, это большинство программного обеспечения, так что я не думаю, что есть разногласия по этому поводу. Не вижу их.

Однако когда речь заходит о DoT или DoH, мы видим, как люди иногда поднимают бровь. «О, вы собираетесь затронуть эту тему? Будете ли вы упоминать это как передовой опыт или нет?». В листе рассылки до сих пор не было твердых доказательств [неразборчиво] по этим двум вопросам, особенно по DoT, но я хотел бы услышать, что люди могут думать о конфиденциальности, с точки зрения рассмотрения конфиденциальности, DoT и DoH. Кто-то поднял руку. Ульрих поднял руку. Может кто-нибудь дать ему... включить его микрофон, чтобы он мог говорить?

УЛЬРИХ ВИССЕР (ULRICH WISSER): Здравствуйте! Это Ульрих. Да. Спасибо, Адиэль, за что предоставил возможность выступить. Я хотел сказать, что я думаю... DoT решает некоторые вопросы конфиденциальности, потому что, очевидно, он не позволяет людям [неразборчиво] прослушивать ваш запрос, но вы все равно должны доверять своему оператору. Это, очевидно, можно решить только с помощью Oblivious DNS, но я не думаю, что Oblivious DNS сейчас близка к передовой практике.

АДИЭЛЬ АКПЛОГАН: Я согласен.

УЛЬРИХ ВИССЕР (ULRICH WISSER): Но я думаю, стоит упомянуть, что DoT решает некоторые проблемы конфиденциальности, но далеко не все.

АДИЭЛЬ АКПЛОГАН: Спасибо. Очень полезный отклик с точки зрения оператора. Упомянутое вами важно и интересно. Доверительные отношения, которые уже каким-то образом существуют между пользователем резолвера и провайдером. Например, в контексте интернет-провайдера очевидно, что существует соглашение об оказании услуг. Существуют некоторые ограничения, которые могут заставить в некотором смысле отодвинуть рассмотрение конфиденциальности, или если вы [неразборчиво], где у вас есть политика, которая заставляет вас использовать резолвер вашей компании, аспект конфиденциальности немного смягчается, потому что в любом случае вы используете корпоративную сеть, поэтому вы должны придерживаться определенной политики.

Но когда вы находитесь в дикой природе, на открытом пространстве, возможно, именно там конфиденциальность становится более важной, и поэтому мы отнесли рассмотрение конфиденциальности... мы пытаемся отнести рассмотрение конфиденциальности к категории, охватывающей публичную и открытую сторону резолвера, где любой может использовать

любой резолвер, и именно там они могут быть обеспокоены конфиденциальностью и тем, что они подписывают для резолвера.

У кого-нибудь еще есть чем поделиться по аспекту резолвера или по [неразборчиво], конечно же, по KINDNS и передовой практике, которую мы изучаем?

Хорошо. Если нет других вопросов или комментариев, это означает, что мы в... Я читаю, что мы действуем в правильном направлении. Я хотел бы поблагодарить всех, кто присоединился к листу рассылки и внес свой вклад в эту инициативу. Кажется, есть один вопрос. А, есть один вопрос в модуле. Я его пропустил. Не могли бы вы зачитать его?

КИНГА КОВАЛЬЧИК (KINGA KOWALCZYK): Да. Итак, является ли измерение частью KINDNS, формой измерения, где сообщество может оценивать данные резолверов, различных резолверов, и имеет способ сравнения? Является ли измерение частью KINDNS?

АДИЭЛЬ АКПЛОГАН: Как я уже говорил, мы определим индикатор, который позволит нам увидеть, как это влияет на некоторые аспекты безопасности DNS в целом. Какие это будут показатели, пока четко не определено. Мы также можем использовать некоторые из этих идентификаторов из других инициатив ICANN, таких как [ITHI],

например, или другие измерения, инициативы, которые уже существуют.

Но в заданном здесь вопросе есть упоминание об оценке любых данных резолвера. Я не знаю, какого рода данные здесь используются и насколько они уместны в данном конкретном случае.

Обычно, с нашей точки зрения, когда мы измеряем подобные вещи, мы стараемся измерять то, что мы можем измерить с нашей точки зрения, не пытаясь получить доступ к частным данным, которые мы не контролируем. И мы, вероятно, будем измерять эти вещи в соответствии и только в связи с передовыми практиками, которые мы имеем в нашей [неразборчиво] может быть в состоянии сказать, ну, количество резолверов, которые имеют проверяют конфиденциальность [неразборчиво] весь этот путь за последний месяц, год или около того путем измерения тех из резолверов, в которых работают DoT или DoH или QName Minimization. Это способ, с помощью которого мы можем измерить это напрямую.

Но я не знаю, что вы имеете в виду под оценкой данных резолвера, потому что когда вы начинаете говорить об оценке данных резолвера, это дает мне совершенно другой взгляд на это. Мы будем измерять то, что мы можем видеть публично, но только в отношении передовых практик, которых мы ранее [придерживались].

Кроме того, мы хотим привлечь как можно больше специалистов по решению проблем, чтобы они присоединились к инициативе и взяли на себя обязательства по внедрению передового опыта. Если в ходе этого нам удастся найти способ сотрудничества и работы с некоторыми резолверами для проведения расширенных измерений и расширенного изучения того, что они видят, то, конечно, это может быть добавлено к инициативе.

Но опять же, мы сделаем это как можно проще, чтобы предлагаемое нами не вызывало никаких противоречий как у пользователей, так и у людей, которые будут [неразборчиво] следить за результатами инициативы.

Хорошо. Лист рассылки открыт. Присоединяйтесь, и мы сможем продолжить некоторые из этих обсуждений там. Вы можете обсудить там другие соображения или вопросы, которые у вас могут возникнуть, или обратиться непосредственно к нам в OCTO. Вы также можете написать непосредственно на OCTO@ICANN.org, если у вас есть прямой вопрос.

И я вижу вопрос от Дезирэ. Спасибо, Дезирэ. Да. Как я уже упоминал, здесь есть компонент коммуникации и информирования, который также очень важен. Конечно, мы работаем с сообществом в целом. Но именно поэтому у нас где-то там есть программа послов, где мы будем работать с сообществом и продвигать это. Но ICANN также выделит определенные ресурсы на информирование и продвижение инициативы, как только мы

объявим о ее запуске. Конечно, успех будет в значительной степени зависеть от продвижения, возможно, и от того, как мы сделаем это легко доступным и удобным для потребления.

Спасибо всем за участие. У нас осталось всего девять минут отведенного на это времени. Я не вижу больше вопросов, но надеюсь, что мы встретимся со всеми участниками листа рассылки в оффлайне, чтобы обсудить это. Что-нибудь еще, Кинга, о чем нам нужно поговорить? Если нет, снова вам слово.

КИНГА КОВАЛЬЧИК: Нет, мы ответили на все на вопросы. Спасибо всем. Презентация будет опубликована также на сайте ICANN73, вероятно, через пару дней. Спасибо.

АДИЭЛЬ АКПЛОГАН: Спасибо, Кинга. Спасибо, Стивен. Вам тоже спасибо, Фил. Всем до свидания.

ФИЛ РЕНО: Спасибо.

[КОНЕЦ СТЕНОГРАММЫ]