ICANN83 | Форум по вопросам политики – Заседание GAC по вопросам безопасности и стабильности
Среда, 11 июня 2025 г. – с 09:00 до 10:15 CEST

DAN GLUCK

Приветствуем вас на заседании GAC в рамках ICANN83, посвященном вопросам безопасности и стабильности, которое имеет место в среду, 11 июня, в 07:00 по Гринвичу. Обращаем ваше внимание, что это заседание записывается и проводится в соответствии с ожидаемыми стандартами поведения ICANN и политикой ICANN по борьбе с домогательствами. Во время этого заседания вопросы или комментарии будут зачитываться вслух только в том случае, если они были представлены в надлежащей форме в чате Zoom. Устный перевод на этом заседании будет осуществляться на всех шести языках ООН и португальском языке.

Если вы хотите выступить в ходе этого заседания, пожалуйста, поднимите руку в зале Zoom. Когда вас вызовут, участникам будет разрешено включить звук в Zoom. Пожалуйста, назовите свое имя для протокола и язык, на котором вы будете выступать, если это не английский, и говорите в умеренном темпе, чтобы обеспечить точность устного перевода. Сейчас я передаю слово заместителю председателя GAC Марко Хогевонингу (Marco Hogewoning). Спасибо, вам слово.

MARCO HOGEWONING

Спасибо, Дэн. Доброе утро всем. Действительно, я буду председательствовать на этом заседании, и надеюсь, что наш уважаемый председатель Нико находится где-то в зале и наслаждается чашечкой кофе. Как вы видите, мы разделили это заседание на две части. Сначала SSAC расскажет нам о некоторых проектах, над которыми они будут работать, а затем я попросил Кристиана Хессельмана (Cristian Hesselman) из SDNLabs рассказать нам немного больше о том, как квант взаимодействует с DNSSEC, в продолжение заседания, которое мы провели в Сиэтле на ICANN82.

Прежде чем мы начнем, возможно, стоит быстро представиться тем, кто сидит за столом. Дэн уже представил меня. Я Марко Хогевонинг (Marco Hogewoning), представитель GAC от Нидерландов. Возможно, Маартен, вы хотите начать?

MAARTEN AERTSEN

Доброе утро. Меня зовут Маартен Аертсен (Maarten Aertsen), я член SSAC.

WARREN KUMARI

Здравствуйте, я Уоррен Кумари (Warren Kumari), также член SSAC.

GREG AARON

Я Грег Аарон (Greg Aaron) из SSAC.

RAM MOHAN Я Рам Мохан (Ram Mohan). Я также представляю SSAC и являюсь председателем SSAC.

CRISTIAN HESSELMAN Кристиан Хессельман (Cristian Hesselman). Я работаю в SIDN, регистратуре домена верхнего уровня .NL, Нидерландов.

MARCO HOGEWONING Спасибо. Тогда, без лишних слов, я передаю слово Раму для обсуждения нашей первой темы – регистрации доменов.

RAM MOHAN Спасибо, Марко. Перейдем к следующему слайду. Мы хотели бы поделиться с вами некоторыми комментариями по поводу доступа к регистрационным данным доменов. Следующий слайд, пожалуйста. Мы хотели бы, чтобы GAC знал о нашей цели. Мы хотим убедиться, что любые политики доступа к регистрационным данным gTLD четко определены, надежны и отвечают потребностям глобального интернет-сообщества в защите от угроз безопасности. Это то, что мы решаем.

Мы считаем, что для этого необходимо создать систему доступа, которая будет следовать структурированному и ускоренному механизму, так чтобы законные запросы, особенно срочные, обрабатывались в приоритетном и ускоренном порядке. Политика в отношении времени

реагирования, политика в отношении того, как, что и когда, все эти элементы должны быть четко определены и приняты сообществом. Мы также считаем, что корпорация ICANN должна продолжать предоставлять статистику по запросам данных, поступающим для регистрации доменов.

Мы считаем, что доступ к регистрационным данным важен. Это фундаментальная часть безопасности и стабильности. Мы предоставили EPDP свои комментарии по этому вопросу, но хотим сказать, что это не противоречит требованиям конфиденциальности. Необходимо надлежащим образом учитывать потребности в конфиденциальности, но существует явная обеспокоенность по поводу безопасности и стабильности. И так что мы хотим убедиться, что процесс, с помощью которого эти изменения будут внесены в сообщество, будет учитывать принципы, которые мы перечислили здесь, на экране. Вот что мы хотели сказать. Мы открыты для любых вопросов или комментариев.

MARCO HOGEWONING Спасибо, Рам. И, конечно, да, я думаю, что GAC согласен с вашими замечаниями о доступе к регистрационным данным. Есть ли вопросы? Нет, еще рано. Я не вижу ни одного в Zoom. Я не вижу ни одного в зале. Ну, возможно, в конце заседания мы сможем вернуться к этому вопросу. Но следующая тема, я полагаю, будет посвящена программному обеспечению с открытым исходным кодом. Маартен?

MAARTEN AERTSEN

Да. Мы работаем над темой, которая, возможно, знакома некоторым из вас, а именно над свободным и открытым программным обеспечением, которое можно свободно использовать, распространять, изменять и изучать. Мы специально анализируем роль этого типа программного обеспечения в глобальной системе DNS. Мы полагали, что от него зависит очень многое, но в этом сообществе не было проведено ни одного обширного исследования.

А свободное программное обеспечение с открытым исходным кодом имеет довольно уникальные характеристики с точки зрения разработки и управления. И пока во всем мире люди обсуждают инфраструктуру, надежность, программное обеспечение и т. д., мы сочли полезным сделать видимой роль этого типа программного обеспечения, его характеристики, чтобы убедиться, что при обсуждении политики это будет принято во внимание. Так что у этой работы две цели. Мы хотим показать эту критическую зависимость. Мы хотим показать особенности этого программного обеспечения и, возможно, сообщить о некоторых предположениях, которые логично было бы сделать в отношении программного обеспечения в целом, но которые могут не соответствовать действительности в случае этого конкретного типа программного обеспечения. Таким образом, это своего рода анонс презентации.

Следующий слайд, пожалуйста. Мы рассматриваем в основном четыре области. Мы проводим опрос, в котором описываем состояние дел. Мы рассматриваем регистрацию доменов. И мы рассматриваем DNS, где люди публикуют и получают отображения, что дает вам представление о состоянии дел в мире. Мы анализируем характеристики этого программного обеспечения, включая его модель разработки, которая отличается от той, которую вы могли бы предположить для физических товаров или другого программного обеспечения. Затем мы сравниваем в рамках этой области свободного и открытого программного обеспечения, насколько эти общие характеристики применимы к программному обеспечению, которое популярно в DNS, то есть к программному обеспечению, которое нас интересует в данном контексте.

Затем, в третьей части мы разъясняем предположения, которые, как мы видели на практике, не подтверждаются, и выясняем, где есть неверные представления. И, наконец, мы пытаемся перечислить соответствующие факторы риска, которые необходимо учитывать при разработке политики или регулирования. Они касаются не только разработки, но и эксплуатации этого программного обеспечения. Так что, в основном, это те области, которые мы охватываем.

Следующий слайд. В Маскате мы, возможно, расскажем вам об этом подробнее, поскольку надеемся опубликовать этот отчет в течение нескольких месяцев после сегодняшнего

мероприятия. В качестве небольшого анонса скажу, что мы считаем использование свободного и открытого программного обеспечения в DNS и регистрации доменных имен сильной стороной, но есть и риски, которые необходимо учитывать. Мы считаем, что можем предложить некоторые рекомендации в этом отношении, касающиеся использования свободного и открытого программного обеспечения. На сегодня все. Я готов ответить на ваши вопросы.

MARCO HOGEWONING Это действительно короткий и лаконичный анонс. Есть ли вопросы к Маартену об этой работе? Я оглядываюсь по сторонам. Вижу, что Индия снова поднял руку.

SAJID Спасибо, председатель. Саджид из Индии. Мой вопрос на самом деле к г-ну Раму Мохану (Ram Mohan). Вы пропустили это из-за нехватки времени. У нас общая цель — регистрационные данные должны предоставляться в течение 24 часов, но уже более 24 месяцев мы пытаемся добиться от ICANN соглашения о сроках, не говоря уже о 24 часах. Я имею в виду любые сроки. На данный момент у нас нет никаких сроков по этому вопросу.

Таким образом, несмотря на то, что GAC и SSAC неоднократно заявляли о срочности решения, из-за затянувшегося процесса, я думаю, что сейчас дело идет по двум

направлениям: одно касается аутентификации, а другое — политики. Что вы думаете, как председатель SSAC и, возможно, вопрос заместителю председателя GAC, будет ли полезно совместное заявление SSAC и GAC, чтобы убедить Правление ICANN установить сроки и принять решение по срокам как можно скорее?

RAM MOHAN

Спасибо за выступление. Мы согласны с тем, что для срочных запросов процесс должен быть очень четким. И я полагаю, что некоторые обсуждения уже ведутся со сторонами, которые должны реализовать эти изменения. Я пока не могу говорить от имени всего SSAC. Мне нужно будет проконсультироваться с членами. Но мы достаточно четко заявили, что если что-то названо и признано срочным, то это должно рассматриваться как срочное, и ответы должны быть очень быстрыми. Это не должно занимать много времени. Если совместные действия с GAC помогут, мы будем открыты для этого, чтобы подчеркнуть важность этого вопроса. Мы считаем, что это важный вопрос. Частично это связано с тем, что мы должны четко понимать, что срочное означает срочное, а не обычный ход дела.

MARCO HOGEWONING

Спасибо, Рам, я с вами согласен. Как вы знаете, GAC упоминал о срочных запросах, по крайней мере, в последних пяти коммюнике, насколько я помню, включая некоторые рекомендации. Мы активно, или, по крайней мере, некоторые

из наших коллег активно работают в малых группах, занимающихся этим вопросом. На мой взгляд, работа продвигается. Я согласен с вашим замечанием, что в случае срочного запроса прогресс не идет с той скоростью, которая необходима. И я думаю, что могу с радостью присоединиться к Раму, так что давайте будем иметь это в виду и подумаем, может ли совместная работа помочь продвинуть дело, я с удовольствием рассмотрю эту идею, так что давайте вернемся к этому вопросу позже. Есть ли еще вопросы? Я вижу, что кто-то указывает на меня. Рассел, да, извините.

RUSSELL WORUBA

Спасибо, председатель, и спасибо, уважаемые коллеги из SSAC. Вы делаете отличную работу. Я большой фанат SSAC и благодарю вас за проделанную работу. У меня есть несколько комментариев. Я думаю, что многие страны в регионах с недостаточным уровнем обеспеченности услугами в значительной степени полагаются на открытый исходный код, в основном на BIND, для работы DNS на уровне ccTLD, и теперь, конечно, в условиях меняющейся ситуации, мы с нетерпением ждем результатов этого исследования. Есть ли у вас на данный момент какие-то базовые данные о текущей ситуации, особенно в разных регионах, чтобы мы могли составить представление? Спасибо.

MAARTEN AERTSEN

Спасибо за этот вопрос. Я дам небольшую подсказку. В обзоре ситуации, где мы пытались получить точные данные о том, кто что использует, мы планируем сказать, или в текущем проекте, который не подлежит публикации, говорится, что глобальная DNS работает на программном обеспечении с открытым исходным кодом. Так что это не только вы, и у нас есть статистика, подтверждающая это. Так, например, в сфере ccTLD 20 из 25 ведущих операторов используют это программное обеспечение. Если добавить сферу gTLD, то это 9 из 10. А если посмотреть на систему корневых серверов, то 9 из 12 используют исключительно FOSS.

И я думаю, что одна из ценностей этого отчета заключается в том, что он может показать более широкой аудитории то, что, возможно, некоторые люди, занимающиеся технологиями, знали, что это вещь повсеместная, и мы надеемся раскрыть эту информацию, потому что мы видели, как в некоторых регионах регулируется программное обеспечение, а FOSS остается на втором плане. И поскольку характеристики настолько разные с точки зрения разработки, финансирования и того, кто их использует, это может быть не самой лучшей стратегией. Да.

MARCO HOGEWONING

Спасибо. Я слышал, что Германия тоже в очереди. Руди.

RUDY NOLDE

Спасибо. Руди Нольде (Rudy Nolde) из Германии. Изначально я хотел спросить, какие рекомендации вы можете дать политикам. Затем я увидел ваш последний слайд, на котором говорится, что вы предложите политикам руководящие принципы, и, как мне кажется, вы только что дали небольшую подсказку. Поскольку я очень нетерпелив, возможно, вы могли бы предварительно сказать, в каком направлении будут развиваться эти руководящие принципы или рекомендации для нас, политиков?

MAARTEN AERTSEN

Я не хочу отнимать время у своих коллег, поэтому буду краток. Итак, в настоящее время мы думаем о том, чтобы выявить некоторые из существующих заблуждений. Например, одно из довольно естественных заблуждений заключается в том, что договорные отношения можно использовать в качестве механизма политики. Вы говорите, что регулируете операторов критически важной инфраструктуры в вашем регионе, а они, в свою очередь, предъявляют требования к своим поставщикам, а те, в свою очередь, предъявляют требования к своим поставщикам и т. д.

Это может работать в случае физических материалов и иногда в случае программного обеспечения. Но это не работает, когда программное обеспечение можно скачать из Интернета, потому что в этом случае нет цепочки. Так что это заблуждение, что такой инструмент будет работать, а на

практике он не работает, потому что существует много программного обеспечения, которое разрабатывается и поддерживается специальной группой, но его использование выходит далеко за рамки существования договоров о поддержке или подобных инструментов.

Такким образом, в качестве рекомендаций, я думаю, мы могли бы предложить некоторые соображения по этому конкретному вопросу, например, как поступать с разработчиками в этом отношении или как думать, но также, если вы предъявляете к операторам требования, которые ограничивают их возможность выбирать лучшее в своем классе программное обеспечение, которым вполне может быть этот тип программного обеспечения, то вы можете не достичь той политики, которую надеетесь достичь. Так что, я думаю, это та область, в которой мы будем работать, но я забегаю вперед. Сначала нам нужно опубликовать отчет, а затем я с удовольствием вернусь, чтобы поговорить с вами об этом.

MARCO HOGEWONING Я думаю, мы будем рады, если вы вернетесь к нам после публикации отчета, и продолжим обсуждение этого вопроса. Я вижу, что в очереди больше нет вопросов, и, учитывая время, предлагаю перейти к последней теме SSAC, которая лично мне также очень интересна, а именно к вопросу о повторном рассмотрении блокировки DNS. Грег, вы начинаете?

GREG AARON

Хорошо. Спасибо. Это документ, который является обновлением двух документов, написанных SSAC около 12 лет назад. Таким образом, блокировка DNS — это не что-то новое, но мы решили, что пришло время обновить информацию, потому что в мире появилось много новых примеров блокировки DNS, и мы увидели, к чему приводят эти действия. Кроме того, за это время были разработаны новые технологии, которые влияют на блокировку DNS и на то, как люди могут получать доступ к ресурсам в Интернете. В эту группу вошло около 20 членов SSAC. Уоррен и я были сопредседателями группы.

Итак, что такое блокировка DNS? Когда вы сидите за компьютером и хотите посетить, скажем, веб-сайт, вы вводите адрес, доменное имя, и ваш запрос отправляется на DNS-резолвер. Мы называем их рекурсивными резолверами. Они часто управляются вашим интернет-провайдером. Затем рекурсивный резолвер помогает определить IP-адрес вашего пункта назначения, преобразует доменное имя в IP-адрес, и в конечном итоге DNS определяет, где находится ваш пункт назначения, и позволяет вам связаться с веб-сайтом, который вы хотите посетить.

Обычно этот процесс происходит практически мгновенно. Вы попадаете туда, куда хотите. Однако рекурсивный резолвер

может заблокировать доменное имя. Это означает, что резолвер сообщит вам не то, что вы ожидаете. В основном это делается двумя способами. В первый раз, в первом случае, рекурсивный резолвер может сообщить вам, что доменное имя, которое вы хотите, не существует, хотя на самом деле оно существует. Так что, например, вы пытаетесь зайти на Википедию, но не получаете ответа. Вы не подключаетесь к Википедии. Другой способ заключается в том, что вместо перехода на нужный вам веб-сайт вы перенаправляетесь на другой сайт. Так что, можно сказать, что рекурсивный резолвер сообщает вам нечто неожиданное, а некоторые даже скажут, что он вам лжет. Он не дает вам ответ, который существует в DNS.

Таким образом, блокировка DNS — это техника. Это инструмент. Как и любой инструмент или техника, он может использоваться для различных целей. Его можно использовать умело. Его можно использовать неумело, как молоток. Вы можете использовать молоток, чтобы построить дом. Это замечательно. Но вы можете использовать молоток, чтобы ударить кого-то по голове, что не является хорошей идеей или хорошим использованием. Так что, в основном, это предназначено для того, чтобы люди не могли получить доступ к контенту или использовать какую-либо услугу. Это влияет не только на посещение веб-сайтов, но и на любое использование DNS. Так что это также повлияет на

электронную почту, управление сетью и все остальное, что зависит от DNS.

Следующий слайд, пожалуйста. Итак, если бы DNS-резолвер был Гэндальфом — у нас в SSAC всегда должна быть ссылка на поп-культуру — он бы сказал следующее. Следующий слайд. Итак, блокировка DNS используется для многих различных целей. Поэтому мотивация важна.

Один из способов его использования — обеспечение безопасности. Резолвер может не пропускать людей... О, как драматично. Электричество отключено. DNS-резолвер может быть настроен так, чтобы не пропускать людей на сайты с вредоносным ПО, фишингом или чем-то подобным. Таким образом, это настройка, которая приносит пользу.

И, вероятно, все мы в этом зале в той или иной степени защищены блокировкой DNS.

Например, все веб-браузеры имеют систему, которая выдает предупреждающую страницу и не позволяет вам перейти на известный фишинговый сайт, например, пока вы не решите, что действительно хотите туда перейти. Так что это нечто, что является эндемичным для многих систем, и это довольно повсеместно и, как правило, предназначено для помощи людям и их защиты. И это обычно делается на уровне локальной сети. Итак, вы выбираете провайдера, который поможет вам обеспечить безопасность в вашей сети.

Некоторые люди используют его для контроля контента. Так, например, ваша местная публичная библиотека может не разрешать посетителям заходить на определенные сайты, которые, по мнению сообщества, не должны быть доступны из библиотеки. Например, сайты с азартными играми или порнографией, потому что в библиотеке бывают дети.

Некоторые компании используют блокировку DNS внутри своих компаний, потому что не хотят, чтобы их сотрудники занимались определенными видами деятельности, такими как просмотр социальных сетей или сайтов азартных игр, пока они работают в сети. Так что, опять же, это своего рода локальная настройка, когда компания определяет политику для своего места работы.

Наиболее спорным является использование блокировки DNS для предотвращения доступа людей к контенту, особенно если блокировка осуществляется на национальном уровне.

Другими словами, это запрет гражданам всей страны посещать определенные сайты и просматривать определенный контент. И это одна из причин, по которой мы хотим предоставить эту информацию политикам, членам GAC и другим лицам, поскольку эти решения затрагивают интересы большого количества людей.

Иногда блокировка осуществляется на основании закона. Например, в некоторых странах гражданам запрещено посещать известные сайты, на которых распространяются

изображения сексуального насилия над детьми. Это делается для защиты детей и граждан. У стран есть списки таких доменных имен, которые они распространяют среди интернет-провайдеров. Наиболее спорным является блокировка DNS в некоторых местах для предотвращения доступа к контенту, выражающему политические взгляды. То есть, она используется для цензуры.

Следующий слайд. Мы хотим провести различие между блокировкой DNS и приостановкой доменных имен. Обе эти меры преследуют одну и ту же цель — предотвратить доступ к определенному контенту. Однако блокировка DNS не удаляет контент из Интернета. Если доступ к контенту заблокирован для некоторых пользователей, другие пользователи по-прежнему могут получить к нему доступ. При приостановке домена доступ к контенту блокируется путем отключения доменного имени, чтобы он не работал. В настоящее время из-за проблем безопасности и злоупотреблений, например фишинговых сайтов, ежедневно приостанавливается действие тысяч доменных имен.

Иногда сайты закрываются по решению суда, так что они перестают работать для всех. Правоохранительные органы, например, на этом графике, закрывают веб-сайт в результате судебного решения, чтобы предотвратить преступную деятельность. И они могут либо закрыть его полностью, либо

перенаправить и перенести на новые серверы имен. Это две разные вещи, но они часто используются для схожих целей, чтобы предотвратить доступ.

Следующий слайд. Это примечание из документа. В этом документе SSAC рассказывает о методах, которые используются для блокировки DNS, и о некоторых мотивах. Конечно, люди могут не соглашаться с конкретными случаями. То, что незаконно в одной стране, может быть законно в другой. Люди могут не соглашаться с обоснованностью решения суда о блокировке чего-либо. Мы не выносим суждений по каким-либо конкретным случаям. Следующий слайд.

WARREN KUMARI

Спасибо. Итак, как сказал Грег, блокировка DNS — это инструмент. И, как и любой инструмент, он имеет свои сильные и слабые стороны. Также важно понимать, как работает этот инструмент, чтобы вы могли наилучшим образом понять, как его использовать, и случайно не порезаться при этом.

Итак, блокировка DNS работает путем размещения в рекурсивном резолвере списков того, что должно быть дозволено для разрешения, а что нет. Одним из следствий этого является то, что она применяется только к пользователям, которые фактически используют этот рекурсивный резолвер. Это означает, что, если пользователь

решит использовать другой рекурсивный резолвер, он сможет минуть или обойти блокировку.

На этой схеме внизу пользователь отправляет свои запросы на один из стандартных резолверов своего интернет-провайдера. Если имя, которое он пытается найти, в порядке, то оно разрешается нормально. Но если оно находится в одном из блок-листов DNS, произойдет нечто другое. Вы получите ответ, что имя не существует, или рекурсивный резолвер попытается перенаправить вас в другое место. Но если пользователь не запрашивает этот рекурсивный резолвер, DNS-запросы поступают в другой резолвер, где нет блокировки, и пользователь сможет получить доступ к Интернету в обычном режиме.

Следующий слайд. Так, как же пользователи могут использовать другой резолвер? Один из очевидных способов — это наличие значительного количества так называемых публичных резолверов, которые используются большим количеством пользователей. Исследование APNIC, проведенное Джеффом Хьюстоном (Geoff Houston), показывает, что около 21 % пользователей в настоящее время используют один из известных во всем мире публичных резолверов. Некоторые примеры: Google Public DNS, Cloudflare запускает открытый публичный резолвер, Quad9 тоже, но есть также версии, предоставляемые правительством. Очевидный и хорошо известный пример — DNS4EU, публичный сервис резолверов, спонсируемый

правительством. Таким образом, даже пользователям, не обладающим техническими знаниями, относительно легко обновить настройки рекурсивного резолвера и выбрать один из этих альтернативных DNS-серверов.

Следующий слайд. Если вы в последние несколько лет пользовались каким-либо сервисом потокового вещания, то наверняка видели множество рекламных объявлений о различных VPN-сервисах. Наиболее распространенными из них являются NordVPN и Surfshark, но их существует огромное количество. Они предоставляют пользователям ряд преимуществ. Они повышают конфиденциальность пользователей и обеспечивают большую анонимность, но в своих рекламных объявлениях они также четко указывают, что эти сервисы предназначены для обхода географических ограничений.

Так что, например, если вы путешествуете и хотите посмотреть потоковое вещание в своей стране или контент, доступный в вашей стране, вы можете просто запустить VPN, и теперь для Интернета вы будете как будто находитесь в этой стране. Другой очевидный случай — если вы находитесь в одной стране и хотите посмотреть контент, недоступный в вашей стране, вы можете просто запустить VPN, выбрать конечную точку в любой стране, в которой хотите оказаться, и в Интернете будет выглядеть так, как будто вы находитесь там.

Одно из последствий этого заключается в том, что вы используете другой набор рекурсивных резолверов, и для Интернета вы выглядите так, как будто находитесь не в той стране, в которой на самом деле находитесь. Это означает, что, если в наборе рекурсивных резолверов есть блокировка, вы можете легко обойти ее, просто включив VPN. Следующий слайд. Думаю, слово снова к вам.

MAARTEN AERTSEN

Следующий слайд. Так что же может пойти не так, или, по крайней мере, не так хорошо? Чрезмерная блокировка — это когда блокировка слишком широкая. Например, вы можете заблокировать домен третьего уровня, что более точно, чем блокировка домена второго уровня или блокировка на уровне TLD. Если ваша блокировка слишком широкая, вы можете перекрыть доступ к более чем одному адресу назначения или более чем одному веб-сайту, что доставит неудобства посетителям тех сайтов, которые не представляют собой проблему.

Так что это часто происходит, когда вы блокируете не то место. Кстати, в документе приводится множество примеров из практики, и если вы хотите углубиться в детали, мы рекомендуем вам ознакомиться с этими примерами. В одном случае чрезмерной блокировки, например, в Италии существует система, которая распределяет некоторые доменные имена между интернет-провайдерами, и случайно

они включили в список домен, который использовался для инфраструктуры, и это привело к чрезмерной блокировке, и фактически заблокировало, например, Google Docs для пользователей в Италии на короткое время, пока кто-то не обнаружил ошибку. Так что эта ошибка доставила неудобства людям и помешала им получить доступ ко всему контенту, который не представлял никакой проблемы. Это своего рода побочный ущерб. Если вы делаете это плохо, вы начинаете мешать людям, которым не хотели мешать.

Следующий слайд. Итак, как описал Уоррен, люди могут обойти блокировку. Поэтому, когда происходит блокировка, следует предполагать, что некоторые пользователи обойдут ее, особенно если у них есть для этого мотивация. Они могут использовать VPN. Они могут использовать альтернативные резолверы. На самом деле, существуют другие технологии, которые помогают людям сохранять доступ к контенту или позволяют пользователям получить доступ к контенту. Так что эффективность блокировки DNS часто зависит от степени ее применения. Если кто-то предполагает, что если мы заблокируем домен и отправим распоряжение интернет-провайдерам в нашей стране, то проблема будет решена. Она будет решена для некоторого числа пользователей, но, вероятно, не для всех. Следующий слайд, пожалуйста.

WARREN KUMARI

Так что, когда домен заблокирован, рекурсивный резолвер может ответить двумя общими ответами. Один из них просто сообщает, что доменное имя не существует. Но мы видим, что требуется еще и перенаправление пользователя рекурсивным резолвером в другое место. Похоже, что этот тип блокировки становится все более распространенным. И мы считаем, что это действительно довольно опасно.

Причина этого в том, что, если пользователь пытается зайти на сайт, например foo.bar.com, и его перенаправляют в другое место, в его веб-браузере появится предупреждение о том, что он пытался зайти на foo.bar.com, но веб-сервер, к которому он подключается, не является foo.bar.com. Пользователи привыкнут просто закрывать эти предупреждающие сообщения, а это может иметь серьезные последствия для безопасности. В первую очередь, они просто научатся игнорировать всплывающие предупреждения. И хотя это может произойти с сайтом, заблокированным DNS, в следующий раз это может быть их банк или что-то подобное. Так что, в основном, одна из вещей, о которых говорит Druckmann, это то, что не следует использовать перенаправление, если вы собираетесь блокировать DNS.

И это подводит нас к следующему ряду вопросов, которые, на мой взгляд, являются рекомендациями. Это снова я. Как мы уже неоднократно говорили, блокировка DNS — это инструмент, и, как и любой инструмент, особенно мощный, он может быть использован для добрых дел, но, если вы не

понимаете, как он работает, и не прочитали предупреждающие инструкции, вы можете нанести себе серьезный вред. Так что, если вы собираетесь реализовать или ввести обязательную блокировку DNS, убедитесь, что вы действительно понимаете, как она работает, а также каковы сопутствующие ущерб и побочные эффекты.

MAARTEN AERTSEN Следующий слайд, пожалуйста. Итак, вторая рекомендация SSAC заключается в том, что если вы собираетесь ввести блокировку, будь то в компании, у отдельного интернет-провайдера или на национальном уровне, вам следует следовать этим рекомендациям. Некоторые из них основаны на медицинских рекомендациях «не навреди».

Итак, во-первых, вы должны понять, будет ли блокировка DNS соответствовать вашим целям. Могут быть альтернативные способы решения вашей проблемы. Опять же, например, если вы собираетесь блокировать, у вас могут быть пользователи, которые обойдут блокировку. Поможет ли вам это или этого недостаточно? Во-вторых, у вас должна быть четкая политика относительно того, что вы собираетесь блокировать и как вы собираетесь это делать. И у вас должны быть четко определенные процедуры для проверки того, что попадает в блок-лист, и вы должны минимизировать риски. Вы должны, например, понимать, как исправить ошибку. Мы не рекомендуем конкретные политики и процедуры, потому что

они должны варьироваться в зависимости от ваших целей и задач, но это важный принцип.

В-третьих, реализуйте ее таким образом, чтобы свести к минимуму чрезмерную блокировку или побочный ущерб, который может затронуть ваших пользователей, то есть людей, за которых вы несете административную ответственность. Опять же, например, в компании это ваши сотрудники. И, наконец, вы не должны затрагивать людей, не входящих в сферу вашей административной ответственности. Здесь, в Европе, например, есть много стран. Некоторые интернет-провайдеры в Европе обслуживают клиентов в более чем одной стране. Так что, если вы находитесь в стране A, а интернет-провайдер обслуживает людей в стране A и стране B, что произойдет, если интернет-провайдер получит приказ от страны A заблокировать доступ? Потому что это юрисдикция, в которой находится компания.

Как интернет-провайдер может заблокировать доступ, но не затронуть людей в стране B, которые находятся за пределами юрисдикции? Мы должны помнить, что, когда мы смотрим на глобус, мы видим линии, которые являются нашими национальными границами, но Интернет не совсем соответствует этим линиям. Так что, по сути, мы говорим: будьте осторожны, чтобы не затронуть людей, на которых вы не имеете права влиять. Последний слайд, пожалуйста.

WARREN KUMARI

Я буду очень быстро, потому что у нас нет времени. Последняя рекомендация адресована операторам резолверов, и SSAC рекомендует им использовать этот новый RFC для аннотирования сообщений об ошибках, включая сообщения о блокировке, с указанием причины их возникновения. Переходим дальше. На самом деле, я думаю, что у нас тоже нет времени на вопросы.

MARCO HOGEWONING

Да, у нас очень мало времени, но спасибо. Это очень тщательно проработанная работа. Как часть вашей целевой аудитории, я действительно это ценю. Это дает много пищи для размышлений. У нас мало времени, но я думаю, что можно задать один короткий вопрос. Я уже видел в чате Папуа-Новую Гвинею. Рассел, хотите задать свой вопрос?

RUSSEL WORUBA

Спасибо, Марко. Наша страна получила приглашение принять участие в испытаниях защищенного DNS. Я хотел бы уточнить, действительно ли речь идет именно о защищенном DNS.

MAARTEN AERTSEN

Да, так что защищенный DNS можно реализовать с помощью блокировки DNS. Например, упомянутые нами публичные резолверы занимаются предоставлением защищенного DNS. Они блокируют фишинг и вредоносное ПО, чтобы защитить своих пользователей. Это один из методов, который можно

использовать для защиты людей. Мы также хотим упомянуть, что этот документ уже был использован для обоснования некоторых политических решений, которые в настоящее время обсуждаются в Японии, где рассматривается возможность блокировки очень специфического контента внутри страны.

WARREN KUMARI

И небольшое обновление по этому поводу. Cloudflare — одна из организаций, которая предлагает публичные резолверы. Они предлагают три разных адреса, или, по крайней мере, три из них. Один из них — их стандартный 1.1.1.1, где они вообще не блокируют ничего. Затем у них есть 1.1.1.2, который блокирует вредоносное ПО. И у них есть 1.1.1.3, который является более защищенным DNS, где блокируется вредоносное ПО и контент для взрослых.

Я думаю, что SSAC, или, по крайней мере, возможно, это только мое мнение, если будет предлагаться защищенная служба DNS для большой группы, пользователь должен иметь возможность выбрать, какой уровень защиты он хочет. Если вы родитель, вы, возможно, захотите заблокировать доступ к контенту для взрослых. Так что вы, возможно, захотите выбрать защищенный DNS-сервис, который это делает. Но

если вы взрослый, вы, возможно, захотите иметь возможность видеть этот контент. Так что, я думаю, это вопрос выбора: включить или отключить. И это возвращает нас к тому, о чем мы говорили ранее, что существуют разные типы блокировки и разные группы людей, которых это затрагивает. Если вы сами решили это сделать или выбрали эту защиту, то это, вероятно, более оправданно, чем если эта защита навязана вам кем-то другим.

MARCO HOGEWONING Хорошо. Спасибо, Уоррен. У меня три человека в очереди. Я закрываю очередь. Прошу всех быть краткими. Если мы будем уделять по минуте на каждый вопрос и ответ, то мы не отстанем от графика. Первый, я думаю, ДРК, Блез.

BLAISE AZITEMINA FUNDJI Да, спасибо большое. Блез Азитемина (Blaise Azitemina) из Демократической Республики Конго, для протокола. У меня есть обеспокоенность по поводу VPN. Хотя я очень благодарен за безопасность и защиту, которые могут обеспечить инструменты или средства VPN, но в то же время, с точки зрения государственной политики, я обеспокоен делокализацией. В основном в так называемых развивающихся странах люди используют VPN не столько из соображений безопасности, сколько для того, чтобы скрыть свой адрес, в основном страну, просто чтобы показать, что они находятся в другой стране. И это иногда является нарушением

безопасности или государственной политики для некоторых наших стран.

Мы видели некоторые платформы доставки потокового контента, которые нашли своего рода решение. Когда вы подключаетесь через VPN или прокси, вам обязательно сообщают, что вы не имеете права или у вас нет доступа. Так что же может быть балансом между безопасностью и достоверностью вашего географического положения? Спасибо.

MAARTEN AERTSEN

Я не думаю, что SSAC учел все последствия. Правда в том, что VPN широко доступны и, как и многие другие инструменты, используются как в хороших, так и в плохих целях. Преступники используют VPN, чтобы скрыть свое местонахождение. VPN используют особенности работы Интернета, так что они никуда не денутся. Некоторые компании ведут списки известных IP VPN. Они используют их, например, для оценки риска трафика, поступающего с этих адресов. Так что есть некоторые инструменты для обнаружения и понимания трафика VPN.

WARREN KUMARI

И очень короткое продолжение этой темы. VPN разработаны так, чтобы выглядеть как обычный интернет-трафик. Так что были некоторые места, где пытались запретить их

использование, либо в компании, либо в стране. И, похоже, в итоге они смогли заблокировать крупные VPN-сервисы, но пользователи хотят иметь доступ к контенту, к которому они хотят иметь доступ. Поэтому пользователи переходят на менее известные, менее отслеживаемые VPN, что в конечном итоге может быть для них гораздо более рискованным. Так что, я думаю, всегда нужно иметь в виду негативные последствия, если вы пытаетесь заблокировать технологию, с помощью которой пользователи пытаются получить доступ к контенту, который они хотят. Они найдут способ достичь своей цели, возможно, более рискованным способом.

MARCO HOGEWONING Спасибо, Уоррен. Возможно, позвольте мне ответить на первые два вопроса, а затем вы сможете кратко на них ответить. Так, первый вопрос из Индии. Нам кратко ответить?

SUSHIL PAL Спасибо. Это Сушил из Индии. Как вы думаете, поддерживаемый правительством DNS, как вы сказали, DNS для ЕС, предлагает какие-либо значительные преимущества по сравнению с другими общедоступными DNS? И второй вопрос, да, я думаю, что VPN имеют значение. Да, конечно, при условии, что это известные VPN. Службы безопасности ищут какие-либо способы мониторинга неизвестных VPN?

MARCO HOGEWONING Эшвин? Да.

MAARTEN AERTSEN Все, что я могу сказать о DNS для ЕС, это то, что написано на их сайте. Они сказали, что в основном это было сделано в целях обеспечения суверенитета. Вместо того, чтобы отправлять трафик на крупные коммерческие публичные резолверы, Европа теперь предлагает DNS для ЕС, так что трафик остается в Европе. Так что принимайте это как есть. Ищут ли спецслужбы способы отслеживать неизвестные VPN? Я не знаю.

SUSHIL PAL Это вызывает обеспокоенность у спецслужб?

MARCO HOGEWONING Индонезия, последний.

ASHWIN SASONGKO SASTROSUBROTO Да, спасибо. Я просто хочу услышать ваш комментарий о блокировке, потому что вы упомянули о негативном воздействии блокировки и так далее. Что, если подход заключается не в том, чтобы разрешить всем DNS входить в наше киберпространство, а в том, чтобы разрешить только тем, кому мы хотим? Так что, например, .go.id, хорошо, вам всем разрешено. Хорошо, это .com. Хорошо, этот разрешен, этот разрешен, а остальные не разрешены. Так что вместо

блокировки мы фактически блокируем все и разрешаем только те DNS, которые мы одобряем. Спасибо.

WARREN KUMARI

Я не знаю, возможно ли это. В Интернете миллионы сайтов, так что составить список разрешенных сайтов было бы очень сложно. Но даже если бы вы смогли это сделать, в настоящее время технически невозможно заблокировать весь доступ к DNS. Существует ряд новых технологий, таких как DNS over TLS, DNS over HTTPS, DNS over QUIC, при которых запрос DNS вообще не виден. Он выглядит как любой другой интернет-трафик. Так что единственное, что вы сможете сделать, это просто заблокировать весь доступ в Интернет в вашей стране, отключить страну от Интернета и запретить Starlink и других спутниковых провайдеров. Так что, если вы подключитесь к Интернету, часть DNS-трафика будет проходить, и люди смогут получить доступ к информации.

MAARTEN AERTSEN

Технологии, о которых упомянул Уоррен, в основном связаны с шифрованием и предназначены для защиты личности конечного пользователя, который отправляет запрос. Так что эти технологии являются попыткой обеспечить большую конфиденциальность в Интернете. Спасибо.

MARCO HOGEWONING Извините, это действительно интересная тема, и я вижу, что она вызывает много интересных дискуссий, так что, я думаю, она заслуживает продолжения. Между тем, за нами находится QR-код для полного отчета. Пожалуйста, прочитайте его. Он уже вышел некоторое время назад. На этом я хотел бы поблагодарить Рама, Грега, Уоррена и Маартена. Пожалуйста, оставайтесь с нами. Но без лишних слов я хотел бы перейти к тому, что я назвал продолжением дискуссии о квантовых вычислениях и некоторых рисках, которая состоялась на заседании в Сиэтле. И я хотел бы передать слово Кристиану Хессельману (Cristian Hesselman) из SIDNLabs, который расскажет нам о том, как это влияет на DNSSEC и, в частности, что мы, как представители правительства, можем сделать для смягчения некоторых проблем. Кристиан, слово за вами.

RAM MOHAN Марко, перед этим я хотел бы поблагодарить GAC от имени SSAC. Мы очень ценим наше постоянное взаимодействие и сотрудничество и надеемся на их продолжение. Спасибо.

MARCO HOGEWONING Спасибо. Извините, Рам. Теперь вы, Кристиан.

CRISTIAN HESSELMAN Спасибо, Марко. Хорошо. Итак, как уже сказал Марко, эта презентация посвящена квантовым компьютерам и DNSSEC, а также тому, какое влияние эти машины будущего могут

оказать на нашу жизнь. В конце доклада я включил несколько предложений для GAC с точки зрения правительства. Слайды пропали. Но ничего страшного. Я просто продолжу. Итак, картинка, которую вы видели, взята из вычислительного центра Лейбница в Германии, где работают над этими квантовыми компьютерами. Но я бы не сказал, что это научная фантастика, но они все еще находятся в экспериментальной фазе. Так что речь идет о долгосрочных исследованиях. Хорошо, мы вернулись. Спасибо.

Следующий слайд, пожалуйста. Хорошо. Итак, прежде всего, каковы ожидания от квантовых компьютеров? И я должен добавить, что я не эксперт в области квантовых компьютеров. Я эксперт в области распределенных систем. Так что, я думаю, что квантовые компьютеры или экспертиза в области квантовых компьютеров в основном относятся к сфере физиков, а я не отношусь к их числу. Так что это то, что я прочитал в литературе. Так что ожидания от квантовых компьютеров связаны с новыми заявками, такими как новые методы открытия лекарств, улучшенное машинное обучение или разработка революционных материалов.

Но, как уже упомянул Грег, технологии можно использовать по-разному. Так что это тот самый молоток, о котором говорил Грег, который можно использовать в позитивном ключе, но он также таит в себе определенные риски. Так что,

обратной стороной квантовых компьютеров является то, что они могут взломать существующие криптографические алгоритмы, которые мы используем. Одним из них могут быть алгоритмы для DNSSEC, которые используются для аутентификации сообщений DNS и проверки целостности этих сообщений.

Слайды снова пропали. Вы хотите, чтобы я продолжил или подождем, пока слайды снова появятся? Хорошо. Мы вернулись. Хорошо. Итак, риск квантовых компьютеров для DNSSEC заключается в том, что они могут потенциально взломать криптографические алгоритмы, которые DNSSEC использует для проверки подлинности и целостности ответов DNS. Таким образом, потенциально злоумышленник может переподписать сообщения DNS с помощью скомпрометированного ключа, а затем сделать вид, что сообщение является подлинным и пришло из надежного источника. В результате люди окажутся на неправильном сайте, или программные компоненты окажутся на неправильном сайте.

Я должен добавить, что мы здесь исходим из того, что уже живем в постквантовую эпоху. Так что это не сейчас, а в будущем. И это не атака типа «запиши сейчас, расшифруй позже», а действительно атака, при которой можно практически в реальном времени расшифровать или скомпрометировать ключи в DNSSEC. Но эксперты считают,

что это произойдет не раньше, чем через 10–15 лет. Так что вы можете спросить: зачем нам заниматься этим сейчас?

Следующий слайд, пожалуйста. Дело в том, что добавление новых или замена существующих алгоритмов шифрования в DNSSEC занимает очень много времени. На этом графике, взятом из одного из документов, показан процесс разработки алгоритма шифрования в DNSSEC. От первого чернового варианта в IETF до существенного уровня внедрения справа. Как видите, это занимает примерно 10 лет. Я думаю, что это характерно для обновлений инфраструктуры. То же самое касается внедрения новых алгоритмов DNSSEC. Так что, если квантовые компьютеры станут реальностью через 10–15 лет, нам лучше уже сегодня подумать о том, что делать с DNS.

Хорошо. Следующий слайд, пожалуйста. Помимо временного аспекта, в настоящее время также важное значение имеет внедрение DNSSEC. Слева вы можете видеть, какие страны подписали свои ccTLD с DNSSEC. Зеленым цветом отмечены страны, в которых он фактически используется, зеленым и синим. Это примерно 48% стран мира. И, как вы видите справа, это проверка. Это карта, на которой больше красного и желтого цветов. Это потому, что проверка этих подписей имеет более низкий уровень внедрения. Так что здесь еще есть над чем работать. Но, как вы видите, в настоящее время развертывание DNSSEC идет полным ходом. Так что это своего рода комбинация с квантовыми компьютерами, особенно если предположить, что в будущем валидация будет расти, а

также что в будущем будет расти и подписание, показанное слева.

Следующий слайд, пожалуйста. Итак, если вы хотите защитить DNS от квантовых компьютеров, мы выделяем три стратегии для этого. Одна из них — это то, что мы называем замена, перепроектирование и вывод из эксплуатации.

Замена означает замену существующих алгоритмов шифрования в DNS на новые, которые являются безопасными в постквантовом мире. Перепроектирование означает полную переработку системы DNSSEC, что является вторым вариантом в таблице. И третий вариант — это вывод из эксплуатации, то есть полный отказ от DNSSEC.

Все эти три подхода имеют свои преимущества и недостатки.

Так, например, стратегия замены относительно проста в реализации. Она стандартизирована, но имеет операционные риски. Об этом я расскажу чуть позже. Перепроектирование — это фактически подход к DNSSEC с чистого листа, при котором используются новые технологии, такие как деревья Меркла. Это снизит операционный риск, но потребует капитальной переработки всей системы и протоколов DNSSEC. Так что это займет много времени.

А затем «Вывод из эксплуатации» — это может звучать просто, но также будет иметь последствия, потому что, избавившись от DNS, вы открываете его для всех видов атак, от которых

DNSSEC пытается защитить. Кроме того, это может повлиять на протоколы, которые зависят от DNSSEC. Поэтому в нашей работе в SIDN мы выбрали первый вариант, то есть замену. Поэтому первая строка выделена зеленым цветом.

Следующий слайд, пожалуйста. И я буду говорить об этом конкретном подходе с этого момента. Я не буду объяснять эту схему, так что не бойтесь. Но то, что вы видите здесь, это взаимодействие между резолверами и авторитетными серверами имен с отображением сообщений DNSSEC. Сообщения с красными и желтыми значками содержат ключевой материал, то есть подписи или открытые ключи, и именно их необходимо обновить.

Следующий слайд, пожалуйста. И чтобы вы могли представить, как выглядят эти подписи, вот два примера. Итак, вверху есть два текущих, слева — открытый ключ. Итак, слева серым цветом обозначен открытый ключ, подписанный текущим, извините, текущим ключом, который мы используем в DNSSEC. А справа серым цветом — подпись, сгенерированная этим ключом. А синим цветом вы видите открытый ключ и подпись, созданную постквантовым алгоритмом, то есть алгоритмом, достаточно сильным для защиты от квантовых компьютеров. Как вы видите, они значительно длиннее. Хорошо. Так что это просто для того, чтобы дать вам представление о том, как это выглядит с технической точки зрения.

Следующий слайд, пожалуйста. Итак, в настоящее время разрабатываются различные квантово-безопасные алгоритмы, как правило, в рамках конкурса NIST PQC. Это Национальный институт стандартов и технологий США. Они организовали конкурс для криптографов, чтобы те разработали алгоритмы, способные противостоять квантовым компьютерам. Мы экспериментировали с некоторыми из них. Как вы можете видеть в этой таблице, примерами являются MAYO Falcon и SQSign.

Имена довольно необычные, и их еще больше. Но мы экспериментировали с этими алгоритмами и проверили время, необходимое для подписания файла зоны. Например, для зоны .nl для проверки записей DNS. Мы также рассмотрели размеры подписей и ключей, потому что на предыдущем слайде вы видели, что они довольно сильно различаются или могут сильно различаться. И, как вы можете видеть из этой таблицы, это своего рода компромисс, потому что если вы используете, скажем, небольшие размеры подписей, вы получаете — если вы используете небольшие размеры ключей, то скорость подписи может увеличиться, и наоборот.

Следующий слайд, пожалуйста. Вот. Итак, это первый эксперимент, который мы провели для зоны .nl. Мы попробовали подписать зону с помощью двух постквантовых криптографических алгоритмов. Это Falcon и MAYO. Вы можете увидеть их справа на рисунке. Я не буду вдаваться в

подробности, но здесь вы можете видеть, что для подписания зоны с помощью этих алгоритмов PQC требуется примерно в два раза больше времени. Обычно на подписание зоны .nl уходит около 10 минут, а с этими алгоритмами PQC — 20 минут. Так что это еще вполне приемлемо. Такие результаты вполне удовлетворительны с операционной точки зрения.

Следующий слайд, пожалуйста. Итак, это то, на чем мы сейчас находимся в SIDN. Мы определили несколько дополнительных задач, которые хотели бы рассмотреть в будущем, и которые в основном связаны с размером этих подписей и открытых ключей. Мы также хотели бы более подробно изучить время проверки на резолверах, например, в сочетании с ролью кэширования. Да, я видел это. Спасибо.

Итак, на последнем слайде представлены несколько предложений для GAC. Возможно, вы могли бы сотрудничать с NIST, правительственным агентством США, чтобы изучить, как мы могли бы согласовать разрабатываемые ими алгоритмы PQC с требованиями DNS. Я знаю, что эти люди заинтересованы в этом конкретном случае использования. Еще одним потенциальным действием могло бы быть стимулирование разработки программного обеспечения с открытым исходным кодом, которое бы интегрировало алгоритмы PQC в инфраструктуру DNS. Возможно, это можно сделать с помощью таких фондов, как NLnet или Sovereign Tech

Fund. По крайней мере, это два фонда, о которых я знаю, которые могли бы спонсировать такую работу.

Возможно, также стимулировать внедрение. Это можно сделать, например, через сайт internet.nl, где можно проверить свойства доменных имен или свойства вашего интернет-соединения. Можно было бы также добавить проверку готовности вашего доменного имени к PQC. И, наконец, немного дополняя предыдущий слайд, мы также должны провести дополнительные исследования операционного воздействия этих новых алгоритмов PQC, если мы будем следовать стратегии замены, и того, что это означает для DNS и его операторов, например, для корневой зоны.

Хорошо. Следующий слайд, пожалуйста. Итак, программное обеспечение, которое мы разработали, и эксперименты, которые мы провели, были выполнены на тестовой платформе, которая является открытым исходным кодом. Программное обеспечение можно загрузить с нашего сайта. Вот QR-код. Если у вас есть дополнительные вопросы, вы можете связаться со мной. Это был мой последний слайд.

MARCO HOGEWONING Спасибо, Кристиан. Так что мы все можем просто скачать какое-нибудь квантовое программное обеспечение и поиграть с ним, или квантово-безопасное программное обеспечение. Здорово. Да, нет, спасибо. Мой главный вывод

заключается в том, что у нас есть действия. С точки зрения правительства Нидерландов, мы начинаем заниматься управлением активами, как вы кратко показали. DNS, как также прозвучало в презентации Уоррена, DNS есть везде. А это значит, что DNSSEC тоже везде. А это значит, что криптография, по сути, присутствует во всем. Так что мы уже активно работаем над тем, чтобы составить список, где она находится на случай, если нам понадобится ее заменить. И я могу сказать по опыту, что это легче сказать, чем сделать. На этом у меня два вопроса. Здесь со мной Барри, а онлайн — Питер. Сначала я дам слово Барри.

BARRY LEIBA Спасибо. Это Барри Лейба (Barry Leiba) из SSAC. Я хотел бы внести одно уточнение, которое я замечаю всякий раз, когда мы говорим о постквантовой криптографии, и которое необходимо подчеркнуть: существует заблуждение, что квантовые компьютеры ставят под угрозу все наши системы шифрования. Я хотел бы пояснить, что, когда Кристиан говорил о подписании и подписях, он имел в виду особый вид шифрования, который подвергается риску со стороны квантовых компьютеров. Общее шифрование, которое мы используем для шифрования трафика в Интернете, не подвергается риску. Речь идет конкретно о типах шифрования, которые используются для цифровых подписей

и обмена ключами. И именно поэтому мы всегда подчеркиваем эти вопросы, когда говорим об этом.

CRISTIAN HESSELMAN Да. В частности, DNS имеет особые требования, поскольку все должно помещаться в пакет UDP, например. И это случаи использования, которые не учитываются специалистами NIST. Так что было бы интересно связаться с ними и предложить им учесть этот, я бы сказал, критически важный случай использования.

MARCO HOGEWONING Спасибо. И, кажется, Питер онлайн. Питер Томассен (Peter Thomassen)?

PETER THOMASSEN Ну, на самом деле, я здесь. Здравствуйте. Питер Томассен (Peter Thomassen). Я член SSAC. Я бы хотел добавить один аспект. Относительное количество подписей DNSSEC на самом деле невелико, например, 5% в домене .com. Но если рассматривать абсолютные цифры, то это все равно более 10 миллионов доменов. И это значительное число. И, конечно, пока неясно, каким будет метод подписи в будущем, когда DNSSSEC должен будет перейти на постквантовые методы. Но очевидно, что какой-то переход будет. И теперь, когда подписано более 10 миллионов доменов, а возможно, к моменту перехода их будет еще больше, будет сложно

провести такой переход без хорошей координации. Так что важно, чтобы это поддерживалось автоматизацией.

И на карте, которую вы показали, не обязательно туда заходить, но на карте было несколько синих стран. А в синих странах есть ccTLD, которые поддерживают автоматизацию таких изменений. Так что нужно подумать, хочет ли ваша страна, я имею в виду конкретно вашу, но и любая другая страна, добавить поддержку таких автоматических переходов. И SSAC, я полагаю, будет рад продолжить обсуждение любого такого аспекта. Так что просто обратитесь ко мне или к любому другому члену SSAC, если вас это интересует.

CRISTIAN HESSELMAN Это отличный аргумент. Спасибо.

MARCO HOGEWONING Спасибо. У нас еще есть немного времени. Так что, если есть еще вопросы. Нико, господин председатель, Вам слово.

NICOLAS CABALLERO Спасибо. Спасибо вам большое. И спасибо за прекрасную презентацию, Рам, и вашей команде. Всегда рад видеть вас здесь. Итак, очень быстро два вопроса. Во-первых, Рам, Кристиан, если мы можем организовать, воспользовавшись тем, что в зале присутствует мой уважаемый коллега Джим Галвин (Jim Galvin), если мы можем организовать презентацию для Правления в Маскате, в Омане, которая

состоится в октябре. Возможно, нам нужно будет подготовить нечто вроде базовой версии, за исключением трех или четырех членов Правления, которые очень хорошо разбираются в технических вопросах. Это, с одной стороны.

С другой стороны, и опять же, пользуясь тем, что я сижу рядом с моими уважаемыми коллегами из Бразилии, мы организуем заседание по наращиванию потенциала для стран Латинской Америки в Сан-Паулу или Бразилиа, нам еще нужно определиться с этим. Но до или после Омана вы могли бы нам в этом помочь? Мы будем говорить в основном о реализации DNSSEC и кратко рассмотрим симметричную и асимметричную криптографию, а также тот факт, что RSA, и я прошу меня поправить, если я ошибаюсь, но, по-видимому, две или три недели назад, я не знаю, наверняка ли это, но, по-видимому, RSA была взломана.

Я не знаю, так ли это на самом деле, но я слышал некоторые истории.

В любом случае, это с одной стороны. С другой стороны, есть много преимуществ открытого программного обеспечения для правительств. Я большой пользователь, активный и быстрый, но мне трудно объяснить простыми словами людям без технического образования преимущества с технической точки зрения, а также с экономической точки зрения, и многое другое о прелестях GPL-2, GPL-3 и лицензий в целом, и почему это хорошо. Так что с вашей помощью и вашим опытом мы

могли бы добиться немного большего успеха. Итак, две вещи: с одной стороны, презентация для Правления, а с другой – помощь в проведении заседания по наращиванию потенциала, регионального заседания по наращиванию потенциала для стран Южной Америки, которое, в данном случае, может состояться в Сан-Паулу или Бразилиа.

RAM MOHAN Нико, спасибо. Мы полностью согласны с обеими идеями и будем рады внести свой вклад в их реализацию. Пожалуйста, свяжитесь со мной, и я с удовольствием помогу в этом.

CRISTIAN HESSELMAN Да, мы тоже.

NICOLAS CABALLERO Извините, но насчет взлома RSA, не могли бы вы?

WARREN KUMARI Да, я подозреваю, что вы имеете в виду статью, недавно опубликованную Google. Это академическая статья, в которой говорится, что планка для взлома RSA была снижена. Это еще не произошло. Просто количество постквантовых криптографических алгоритмов, которые вам понадобятся, извините, сложность квантового компьютера, который вам понадобится, вызывает сомнения. Сколько квантовых битов на самом деле нужно для построения надежной системы?

И в этой статье говорится, что их нужно не так много, как мы первоначально думали, но пока совершенно неясно, как далеко в будущем нам нужно об этом беспокоиться. Если поговорить с разными экспертами, то можно услышать самые разные цифры, но дело не в том, что RSA взломана. Просто, похоже, что в будущем, через несколько лет, ее, скорее всего, взломают. Но реальные оценки сильно разнятся. Я искал страницу, где были приведены средние оценки целого ряда квантовых ученых, и это число колебалось в разных пределах. Но это может произойти завтра. Это может произойти через 50 лет. Это может произойти через 500 лет. Очень трудно предсказать. Скорее всего, это произойдет в ближайшие несколько лет, но, опять же, это одно из тех сложных предсказаний.

Это похоже на термоядерный синтез. Когда-нибудь в ближайшие 20 лет появится энергия термоядерного синтеза, но так говорят уже много лет. Однако сейчас определенно стоит подготовиться, потому что, если это действительно произойдет и RSA будет легко взломана, или любой другой криптографический алгоритм будет легко взломан, нам нужно начать готовиться к этому заранее.

NOCILAS CABALLERO Вы же чините крышу, когда не идет дождь, верно?

MARCO HOGEWONING Хорошо. Спасибо. До кофе осталось две минуты. У меня есть вопрос из Австралии. Предлагаю быстро его рассмотреть. Ингрэм?

INGRAM NIBLOCK Здравствуйте. Спасибо. Я просто задался вопросом по поводу таблицы на предыдущем слайде, где были указаны различные компромиссные решения. Речь идет о размерах ключей, скорости подписи и всем таком. Размер ключей я понимаю, это связано с ограничением размера пакетов UDP. Мне просто интересно, какое практическое значение имеет увеличение времени подписи? Если оно увеличивается, я не помню, сколько вы сказали для .nl, с 2 минут до 10 минут. Это проблема? Вам приходится делать это так часто, что это становится проблемой для DNS?

CRISTIAN HESSELMAN Итак, у нас в зоне 6,2 миллиона доменных имен, и около 60 % из них подписаны, а окно публикации составляет около 30 минут. Так что нам нужно переподписывать каждые 30 минут. Если, допустим, время подписания займет очень много времени, мы можем не успеть. Да. Вот почему мы хотели это знать.

MAARTEN AERTSEN Это также зависит от модели развертывания. Кристиан описывает определенную модель развертывания, в которой

вся зона развертывается за один раз, но есть также модели развертывания, в которых используется поэтапная подпись или даже подпись в режиме реального времени для каждого запроса. Поэтому на этот вопрос трудно ответить в общем, но скорость имеет значение.

PETER THOMASSEN Возможно, главное заключается в том, что чем дольше время подписания, тем больше других изменений необходимо внести в модель развертывания.

MARCO HOGEWONING Спасибо. Надеюсь, это отвечает на ваш вопрос. У нас закончилось время. Рад видеть, что уже назначены первые встречи для продолжения обсуждения. Предлагаю вам найти наших коллег во время перерыва на кофе, если хотите получить дополнительную информацию. Я полагаю, что здесь присутствует немало представителей SIDN, и, конечно же, SSAC также представлен почти в полном составе. Так что еще раз спасибо, Рам, Уоррен, Грег, Маартен и Кристиан, за всю вашу замечательную информацию, за то, что вы провели нас по этому, иногда очень техническому, пути и постарались помочь нам понять, что происходит.

Прежде чем отправить вас на кофе, после кофе через полчаса мы вернемся к заседанию по WHOIS и достоверности данных здесь, в зале GAC. Так что, коллеги из GAC, надеюсь увидеть вас

всех там. Всем остальным надеюсь, что это было информативно. Спасибо за участие и приятного кофе. Спасибо.

[КОНЕЦ СТЕНОГРАММЫ]