اجتماع ICANN73 | الأسبوع التحضيري - مستجدات تبادل المعرفة وتجسيد معايير نظام أسماء النطاقات وأمن التسمية (KINDNS)
الأربعاء الموافق 13 فبراير/شباط 2022 – من الساعة 11:00 إلى الساعة 12:00 بتوقيت الأطلنطي الموحّد

آديل آكيلوغان: سوف نقدم لكم إحاطة موجزة حول تبادل المعرفة وتجسيد معايير نظام أسماء النطاقات وأمن التسمية وهي عبارة عن مبادرة لتعزيز أفضل ممارسات نظام أسماء النطاقات بشكل عام. ولدينا اليوم ترجمة، ومن ثم سوف نطلب منكم استخدام الترجمة. وسوف يتوجب على المتحدث أن يتكلم وينطق ببطء قدر الإمكان بحيث يمكن للمترجمين القيام بعملهم.

اطرحوا أسئلتكم في مربع الأسئلة والأجوبة، بحيث يسهل انتقالها إلينا. وأرى أنه إذا رغبتم في التعليق بصوت عالٍ، فيمكنكم رفع أيديكم وسوف يسمحون لكم بالتحدث. ستيفن، الشريحة التالية، رجاءً.

إذن سوف نجري هذا العرض التقديمي على مرحلتين. سوف أتحدث إليكم من خلال هذه المقدمة الأولى وبعد ذلك سوف أعرفكم [بفيليب رينو] وهو خبير في هذا المشروع وسوف يقدم لكم بعض المعلومات حول ما وصلنا إليه وحققناه حول فحوى وصميم هذا المشروع.

إذن فقد عقدنا جلسة خلال اجتماع ICANN72 حتى قدمنا تعريفًا بمبادرة تبادل المعرفة وتجسيد معايير نظام أسماء النطاقات وأمن التسمية وقدمنا شرحًا موجزًا لما نريد القيام به، ومن ثم سوف أبدأ مباشرة بفحوى وأهداف مبادرة تبادل المعرفة وتجسيد معايير نظام أسماء النطاقات وأمن التسمية. وهي رابطة لمشاركة المعرفة معروفة لدى نظام أسماء النطاقات وأمن [التسمية]. باختصار، هذه المبادرة تتعلق بمشاركة أفضل الممارسات والقدرة على العمل مع المجتمع ومع مشغل نظام أسماء النطاقات بشكل عام من أجل إضافة تعليقهم الطوعي إلى تلك الممارسات المثلى ولكن أيضًا لمساعدتنا جميعًا في ICANN على تعزيز أفضل الممارسات بشكل عام والتأكد من أننا نعمل معًا كما هو معتاد من أجل إبقاء نظام أسماء النطاقات آمنًا قدر الإمكان. الشريحة التالية، من فضلك.

إذن البعض منكم على دراية بالفعل بالمعايير المتفق عليها لأمن التوجيه MANRS وهي عبارة عن مبادرة تدور حول تأمين التوجيه عبر الإنترنت. وتلعب مبادرة تبادل المعرفة وتجسيد معايير نظام أسماء النطاقات وأمن التسمية دورًا ضئيلاً في ذلك بحيث يمكننا القول بأنه إذا كانت لدينا معايير جيدة متفق عليها لأمن التوجيه بالإضافة إلى تبادل المعرفة وتجسيد معايير نظام أسماء

النطاقات وأمن التسمية الجيدة أيضًا، فسوف نقوم بالمزيد من أعمال تأمين الإنترنت وجعله أكثر أمانًا للجميع.

وما نريد تحقيقه هنا مرة أخرى هو تقديم أفضل ممارسات ميسرة للغاية تعمل أو يمكن أن تتبع بسهولة لضمان أن الطريقة التي يعمل بها نظام أسماء النطاقات آمنة ونريد التأكيد أيضًا على عمليات نظام أسماء النطاقات هنا لأن هذه الممارسات المثلى سوف تكون فنية تمامًا فيما يخص تشغيل نظام أسماء النطاقات نفسه. وفي المعتاد، وفيما يخص نظام أسماء النطاقات، تتوفر جميع الخدمات وتتوفر أيضًا التطبيقات العاملة وسوف تحاول المبادرة التركيز بمزيد من التخصيص على تشغيل نظام أسماء النطاقات، أي الجانب الفني في عملية التشغيل.

وإذا كنتم على دراية بنظام أسماء النطاقات، فربما تسمعون حول نظام أسماء النطاقات [يتعذر تمييز الصوت] الذي حدد جميع الممارسات المثلى [يتعذر تمييز الصوت] المرتبطة بنظام أسماء النطاقات وهو ما يزيد كثيرًا عن 2000 صفحة تتحدث حول نظام أسماء النطاقات. إن ما نحاول القيام به هو محاولة إظهار وإبداء -من بين كل هذا- الشيء الأكثر أهمية فيما يقوم أي مشغل بتفعيله في مكونات نظام أسماء النطاقات وما يجب عليه القيم به للحفاظ على أمن نظام أسماء النطاقات. الشريحة التالية، من فضلك.

إذن فقد تمت [ترجمة] المبادرة إلى بضعة مكونات. المكون الأول وهو تحديد وتوثيق معايير الأمن الأكثر أهمية بالنسبة لتشغيل نظام أسماء النطاقات. ويجري القيام بذلك بمساعدة فيل رينو الذي ذكرته لكم سابقًا والمجتمع إلى حد ما لأن لدينا قائمة بريدية يمكننا فيها مشاركة ما يتأتى بشكل منتظم من ذلك العمل الخاص بتحديد المعايير والحصول على التعقيبات والآراء من المجتمع.

وبعد ذلك واستنادًا إلى المعايير المُثلى، فسوف نطلق بوابة مخصصة من أجل نشر أفضل الممارسات بالطبع، وأيضًا من أجل توفير الإرشادات التوجيهية حول كيفية تنفيذها، ولكن أيضًا لتزويد المجتمع بمكان يمكن فيه تقييم معلومات اعتيادية أو مفيدة ويمكن للمشغلين فيه الذين يدعمون المبادرة والملتزمون بتنفيذ تلك الممارسات المثلى أيضًا الانضمام ومساعدتنا على تعزيز أفضل الممارسات كما ذكرت لكم.

إذن سوف يتم نشر [يتعذر تمييز الصوت] كل شيء على موقع الويب المخصص، على اسم النطاق KINDNS.org. وبمجرد القيام بذلك، سوف نبدأ العمل مرة أخرى مع الجميع من أجل تحديد بعض المؤشرات التي قد تساعدنا على رؤية تأثير المبادرة على أمن نظام أسماء النطاقات، وتحديد بعض المؤشرات الأساسية التي يمكنها القياس بمرور الوقت والتعرف على كيفية تطورها في الاتجاه الصحيح أو الاتجاه الخاطئ وإجراء التعديل وفقًا لذلك. وسوف تكون هذه هي المرحلة التالية بعد تنفيذ ذلك.

وفي المعتاد، عندما نقوم بطرح ذلك في سياق ICANN، فإن الانطباع الذي يتبادر إلينا في المعتاد هو: هل سيتناول ذلك وظيفة توفير الخدمات لنظام أسماء النطاقات؟ وهذا يعني أفضل الممارسات للسجل وأمين السجل والمسجل أيضًا.

الإجابة المختصرة هي لا في البداية، لأن هذا وكما ذكرت لكم، يركز ويستهدف الوظيفة الجوهرية لنظام أسماء النطاقات. لكن ربما في مرحلة أخرى من هذا العمل، سوف ننظر في كيفية التخطيط لبعض من تلك الممارسات المثلى بالنسبة لنظام التوفير، بمعنى أفضل ممارسات السجلات وأمناء السجلات وإضافة ذلك إلى المبادرة. لكن هذا بالفعل [يتعذر تمييز الصوت] إلا أن المرحلة الأولى سوف تركز بالأساس على التشغيل. الشريحة التالية، من فضلك.

إذن فقد ركزنا على بعض الفئات. ومرة أخرى، إذا كنت تدير نظام أسماء النطاقات، فإنك تديره في بيئة وهناك مكونات أخرى تسهم في قوة نظام أسماء النطاقات بشكل عام وفي تشغيله الآمن.

وكما ذكرت لكم في البداية، فإننا لن نقوم بتصحيح أي كل شيء، لكننا سوف نركز على مكونات نظام أسماء النطاقات، بمعنى إدارة الخادم الرسمي في بيئات مختلفة، بمعنى نطاقات TLD أو الأشخاص القائمين على إدارة منطقة حرجة يمكن أن يكونوا أيضًا في مستوى ثانٍ. بالإضافة إلى مدير أسماء نطاقات المستوى الثاني عمومًا. إذن لدينا نطاق المستوى الأعلى في منطقة حرجة، مثل [.seal.uk] على سبيل المثال أو أي NIC.TLD مهم وضروري لعمل وتشغيل نطاقات TLD تلك، ومن ثم سوف نضيفها إلى تلك الفئة الأولى. وبعد ذلك الفئة الثانية وهي كل من لديه أي مسجل يدير اسم نطاق في المستوى الثاني.

بعد ذلك، لدينا مشغل وحدة حل تصديق الخادم التكراري عمومًا. وفي تلك الفئة أيضًا لدينا ثلاث فئات فرعية سوف نتناولها: وحدة حل التصديق الخاصة (المغلقة)، ووحدة حل التصديق الخاصة المشتركة، ووحدة حل التصديق العامة.

إذن فإن أفضل الممارسات التي سنقوم بتعزيزها سوف تدور حول تلك الفئات الخمسة. لكن فيما حول ذلك، سوف نوفر إرشادات أيضًا حول كيفية [يتعذر تمييز الصوت] البيئة التشغيلية من حيث الخدمة والنظام والشبكة وتناول بعض اعتبارات الخصوصية أيضًا ذات التأثير على بعض جوانب الأمن عمومًا.

وفي هذه المرحلة، إذا أراد أي من المشغلين الانضمام إلى مبادرة تبادل المعرفة وتجسيد معايير نظام أسماء النطاقات وأمن التسمية والعمل مع هذه المبادرة، سوف يتم تقييمه مرة أخرى—أو تقييمه ذاتيًا مرة أخرى—في مقابل الفئتين الرئيسيتين فقط اللتان ذكرتهما وسوف يتم تعريفهما إما في تشغيل الخادم الرسمي أو تشغيل وحدة حل التصديق عمومًا.

وسوف ننشر بالطبع إرشادات تنفيذ وطرق التعامل وقائمة فحص وعملية التكوين والتجهيز وأمثل إلخ. وثم سؤال هناك حول ماهية البرامج التي سوف نوفر إرشادات توجيهية حولها. وسوف نستخدم أكثرها شهرة، ولكن بالطبع إذا ما قمنا بعرض ذلك بطريقة يفهم الناس بها المفهوم، فيمكنهم تطبيق تلك المفاهيم بسهولة على أي من البرمجيات العاملة هناك. الشريحة التالية، من فضلك.

بداية من الآن، سوف أتيح الكلمة إلى فيليب ليستعرض معكم العناصر المختلفة التي كنا ننظر فيها في تلك الفئات المختلفة. فيليب؟

فيليب رينو: نعم. شكرًا لك، آديل، على المقدمة. هذا مشروع مثير للغاية وأتمنى أن نتمكن من الحصول على بعض التعقيبات والآراء من المجتمع حول مختلف أفضل الممارسات التي نطرحها وقمنا بتعريفها.

وبهذه الطريقة سوف نقسم هذا العمل، أي الطريقة التي نصنف بها أنواع مشغلي نظام أسماء النطاقات، وقد قررنا أن نلاحق ... في البداية، رأينا ربما بعض الأشياء مثل نطاقات المستوى

الأعلى ونطاقات المستوى الثاني. وتبين أنها ربما لم تكن مبسطة إلى حد ما، لكنها كانت أكثر تعقيدًا من ذلك إلى حد ما.

ومن ثم قررنا أن نحدد في البداية ما إن كان أحد سيكون مشغلاً أم لا لأسماء النطاقات الرسمية أو مشغلاً لخوادم نظام أسماء النطاقات ويوفر خدمة وحدة حل التصديق التكرارية.

ولكي نبدأ بالخادم الرسمي، فإن ما قمنا به هو أننا نظرنا في نوع المناطق الموجودة على الإنترنت حسب الطبيعة الهرمية، ونظام أسماء النطاقات بالطبع أكثر أهمية، كلما زاد مستوى التعامل معه بشكل واضح كان الجذر هو الأكثر أهمية وربما الأكثر في عدم الاختراق، عفوًا، لكنه الهدف الأكثر ملاحقة إذا كنتم تنوون تسويته في حالة وقوع حادثة تخص الأمن، فسوف يكون هذا هو الاختيار الأكثر.

وبالتالي، فإن لنطاقات TLD مكانة هامة. لكننا نظرنا أيضًا في نطاقات أخرى قد يكون لها تشغيل هام. على سبيل المثال، إذا ما نظرنا في نفس الخوادم للكثير من الدول، فليس من غير الشائع أن نرى على سبيل المثال في المكان الذي أعيش فيه الآن في الدنمارك (DK)، فإن خوادم الاسم لنظام DK موضوعة في نطاق فرعي يطلق عليه اسم nic.dk. حسنًا، لنقل جدلاً أن نطاقات المستوى الثاني هذه ربما ستكون بنفس أهمية نطاقات TLD التي تقع فيها خوادم الاسم الخاصة بها.

ومن ثم فقد قررنا تقسم هذه الفئات على هذا النحو. المناطق الحرجة، هكذا نطلق عليها. لكن من الواضح أن نطاق المستوى الأعلى عدا جميع المناطق الإضافية أو ما يطلق عليها مناطق الدعم التي تستخدم في توفير خدمة من نوع ما، سواء استضافة خوادم الاسم أو التوابع المماثلة.

وهناك فئة أخرى قررنا إضافتها في المناطق الحرجة وغير مرتبطة ارتباطًا مباشرًا بتشغيل نظام أسماء النطاقات نفسه، لكن إذا ما نظرنا إليها من منظور نطاقات المستوى الأعلى لرموز البلدان أو بعض ملفات المنطقة أو أسماء نظام أسماء النطاقات المرتبطة بتلك القطاعات الهامة، سوف الرعاية الصحية أو الحوكمة الإلكترونية ونظم تحديد خدمات المواطنين، فهناك تلك التي قد تكون أكثر أهمية من غيرها، لكن في هذه الحالة، فقد وضعت مثالاً. ففي الدنمارك، لدينا نظام تحديد هوية وطنية وأنا أدرك أيضًا أنه إذا تعطل نطاق myid.dk، فلن تكون للعديد من الأشخاص القدرة على تسجيل الدخول إلى الإنترنت. وقد تنظرون في مسألة كيفية تأثير ذلك على

نظام أسماء النطاقات، وسوف يقاد ذلك من خلال نموذج التقييم الذاتي وما نريد القيام به حقًا هنا لا يملي علينا بالضرورة ما هي المناطق الحيوية أو غير الحيوية. فهو بالأحرى إطار عمل للأشخاص من أجل تحديد السؤال: هل أنا أدير مناطق حرجة أم لا؟ أو للمؤسسات من أجل تحديد السؤال: هل نحن بصدد تقديم خدمات حيوية؟ ومن ثم، ما هي الإرشادات التوجيهية؟ ما هي أفضل الممارسات التي يجب علينا مراعاتها من أجل حماية هذه الخدمات؟

وبالطبع، لقد قمنا أيضًا بتضمين أشياء مثل التمويل ومواقع الأعمال المصرفية والتي يمكن اعتبارها حيوية من أجل تشغيل وعمل أي اقتصاد وأي دولة.

إذن أؤكد مرة أخرى أن هذا إلى حد ما، لا يمكنني تسميته اعتباطيًا، لكن هذا هو قرارنا في هيكلة ذلك على هذا النحو. كما أنه من حيث نقاط الضعف والتأثير على الدوائر أو الاقتصادات أو الدول، ماذا يحدث لو توافقت أسماء النطاقات هذه بشكل واضح مع نطاق المستوى الأعلى لرمز البلد وكان هو نفسه الأكثر ضرورة؟ الشريحة التالية، من فضلك.

إذن معنا أسماء نطاقات أخرى. وهذا بالطبع جميع أسماء النطاقات الأخرى أسفل نطاقات المستوى الأعلى. كما أنها ضرورية وحيوية أيضًا. وسوف يوفرون جميع الخدمات المتنوعة إضافة إلى مواقع الويب والحوكمة الإلكترونية والتجارة الإلكترونية وجميع الأشياء التي نعرفها على الإنترنت. وهي يجب أيضًا أن تحظى بالإدارة المسئولة أيضًا.

ومن ثم، ليس لأنهم مواطنون من الدرجة الثانية أو أي شيء من هذا القبيل، ولكن لأنه سوف تكون هناك القليل من القيود على نوع أفضل الممارسات التي يتعين علينا مراعاتها والسبب في ذلك أنه يتعين علينا الحصول على هذا التشغيل وربما لتشجيع الناس على البدء في التعامل مع مبادرة تبادل المعرفة وتجسيد معايير نظام أسماء النطاقات وأمن التسمية، والبدء في تنفيذ أفضل الممارسات تلك وألا تحبطهم التعقيدات، ومن ثم إذا كنت تدير نطاقًا من المستوى الثاني، فربما لن يكون لك تأثير كبير على الغير لأنك لا تدير تفويضات ولكن ما يزال لديك -- ربما تتعرض لهجوم إلكتروني. ويمكن أن تتعرض لفشل وتعطل في الأنظمة. وهل تُجري العناية الواجبة؟ هل تدير أفضل الممارسات التي من شأنها السماح لك بالحد من هذه الحوادث أو على الأقل التعافي منها؟

ولا يهم حقًا مدى أهمية النطاق في ذلك الصدد. ويجب على الجميع القيام بذلك لأن النطاق ذي التكون الخاطئ أو النطاق الذي تعرض للقرصنة سوف يؤدي إلى تعطيل بشكل أو بآخر. الشريحة التالية، وتتحدث حول ... نعم.

إذن، مشغلو نظام أسماء النطاقات التكراري. هذا هو الشق الآخر من المنظومة، اتفقنا؟ فقد تناولنا المشغلين الرسميين ومعنا بعد ذلك مشغلو نظام أسماء النطاقات التكراري وهنا توجب علينا النظر في نوع وحدات حل التصديق التكرارية الموجودة معنا.

باختصار، إما أن تكون عامة أو أن تكون خاصة. وعند إلقاء نظرة عن قرب، نجد أنه سوف تكون هناك وحدات حل تصديق خاصة وسوف تكون هذه الوحدات عبارة عن شبكات تابعة لشركات بالكامل، ومغلقة كيًا، ولا يمكن الوصول إليها من الخارج، والوصول إليها يكون من نوع الشبكة الافتراضية الخاصة VPN ودائمًا ما تكون على مساحة عناوين خاصة وسوف تكون هذه عبارة عن شركات ومؤسسات، مثل الرعاية الصحة والبنوك وغالبية شركات الأعمال سوف يكون هيكلها على ذلك النحو. ولكن إلى حد ما، أيضًا الشبكات المنزلية وربما الشبكات الخاصة بأماكن الإقامة.

وبمزيد من الانفتاح، لدينا وحدات حل تصديق خاصة مشتركة وربما يكون الاسم غريبًا إلا أننا نحاول التوصل إلى شيء يمكن -- لم أرد تحديد موفري خدمة الإنترنت الضروريين أو أي نوع من موفري الخدمات. ونحن نقول خاصة مشتركة لأنها خاصة ومقتصرة على مجموعة من العملاء أو مجموعة من المؤسسات ربما. وأنا أتخيل ربما شبكة خاصة بجامعة. ولا يمكن الوصول إليها من الخارج ولكن تستمر مشاركتها من خلال الكيانات المميزة قانونًا ربما. على سبيل المثال، مشاركة العديد من العملاء لوحدة حل تصديق خاصة بموفر خدمة الإنترنت أو ربما تكون في سياق مجموعة متحدة من المؤسسات تحت قيادة فنية واحدة مشتركة.

وسوف تكون عبارة عن فئة واحدة أخرى، وبعد ذلك، سوف يكون لدينا وحدات حل تصديق عامة. وحدات حل تصديق عامة، ونحن نعرفها مباشرة. ونحن نفكر ربما في خدمة 8888 من شركة Google أو Quad9 وهذه الأنواع من الخدمات، ولكن فيما بين ذلك، وخدمة DNS المغلقة حقًا، ولدينا فلترة DNS التجارية التي قد تكون أو لا تكون مفتوحة في شكل واحد لكن - - عفوًا، سوف أحاول التحدث بسرعة أبطأ قليلاً.

بالنسبة لوحدات حل التصديق العامة، فإن لدينا كما ذكرنا لكم شركة Google ومثيلاتها، وبعد ذلك لدينا شبه المفتوحة أو -كيف لي أن أقول اسمها؟ وحدات حل المصادقة المفتوحة ذات المكون التجاري، والتي سوف تحصل من خلالها -مع الاتفاقية أو العقد المناسب- على خدمة إضافية من مشغلي وحدات حل المصادقة الخاصة هذه في صورة خدمات الإجلاء والتصفية أو خدمة DNS الإيجابية والتي يتم فيها تحليل مرور DNS الخاص بك لمعرفة ما إن كان لديك مضيفين مخترقين أو مصابين ببرامج ضارة.

وهذه الأنواع من المشغلين عموميين في العادة ولكن لديهم نوع ما من آليات التحكم في الوصول وربما سداد بعض الرسوم أو إبرام عقد، بحيث أنك قد تستخدم خدمتهم وتستفيد من الإضافة - كيفي لي أن أقول اللفظ المناسب؟ خدمات القيمة المضافة التي سوف يوفرونها.

إذن هذه هي الفئات المختلفة، وفي القسم المحدد أعلاه، فإننا نحدد كيف أن وحدات حل التصديق هذه - كيف يتم تقييد الوصول إلى وحدات حل التصديق هذه؟ فهي ستكون عبارة عن خليط من الوصول إلى عنوان IP أو ربما تكون شهادات أو يمكن أن تكون شبكة افتراضية خاصة. ولا يعنينا ذلك حقًا. ما يعنينا هنا هو أننا نحاول وضع كل واحد من هؤلاء المشغلين في فئة يمكنهم فيها الانطلاق والنظر في مبادرة تبادل المعرفة وتجسيد معايير نظام أسماء النطاقات وأمن التسمية وأن يقولوا "حسنًا، موافقون، هذا ينطبق علينا. ما هي أفضل الممارسات؟"

بالإضافة إلى ذلك وإلى حد ما، ربما بالنسبة للمستخدمين النهائيين والمؤسسات. على سبيل المثال، شركة الأعمال التي تريد البحث، "مرحى، أنا أجري اتصالاً بموفر خدمة الإنترنت. وأنا أستخدم وحدة حل التصديق الخاصة به من أجل توجيه استعلامات DNS الخاصة بي إلى الإنترنت". ما هي أفضل الممارسات التي يجب عليهم مراعاتها وهل هم ملتزمون بها؟ هل يتبعون بالفعل البرنامج؟

ومن ثم يمكنك إحالة موفر الخدمة أو موفر خدمة الإنترنت الذي تتعامل معه أو إدارة تقنية المعلومات. هل نحن نتبع مبادرة تبادل المعرفة وتجسيد معايير نظام أسماء النطاقات وأمن التسمية لأفضل الممارسات الخاصة بوحدة حل التصديق؟ هل نوفر الحماية لخصوصية المستخدمين بالطريقة الموصوفة هنا؟ الشريحة التالية.

إذن التوصيات المقدمة إلى وحدات حل التصديق الخاصة. إننا لم نغطي في حقيقة الأمر الكثير من التوصيات لوحدات حل التصديق الرسمية لكن هذا الأمر غير هام للغاية في الوقت الحالي. فلنركز على الوحدات الخاصة.

وحدات حل التصديق الخاصة، كما ذكرنا لكم، موجودة في الشبكات الخاصة. وهي في بعض الحالات جزء من نطاق منافس ومعتمد مثل الدليل النشط، أو أشياء من هذا القبيل. لذلك سوف نجدها في الكثير من بيئة برنامج ويندوز.

وما الذي قمنا به عندما ركزنا عليها، لقد ركزنا بالأساس على أمن الشبكة وحددنا أيضًا الحاجة إلى الشفافية وهو ما يعني أن بعض التوصيات التي قد تكون معقولة في أماكن أخرى مثل حل نظام أسماء النطاقات عبر بروتوكول نقل النص التشعبي الآمن DoH أو نظام أسماء النطاقات عبر بروتوكول أمان طبقة النقل، والكثير من هذه الشبكات ما يزال غير واثق في تمكين هذه الخدمات لكن ما يزال بإمكانهم الاستفادة من DoH أو DoT، على سبيل المثال، وتوجيه استعلاماتهم إلى وحدة حل تصديق علوية لديها أمن - عفوًا، ذات إمكانية تشفير، بما يتيح لك أن تؤمّن على الأقل التنصت على الاستعلامات في طريق خروجها من الشبكة. إذن هذا سيناريو مختلف قليلاً بالنسبة لكل من المشغلين.

ثم بعد ذلك توافر ومرونة الخدمات. وكما ذكرت لكم آديل، فإن بعضًا من هذه الممارسات المثلى سوف تغطي أفضل ممارسات إدارة الأنظمة الجيدة والقديمة، ومن ثم فلن نتطرق إليها في الوقت الحالي، ولكن سوف يتم ذكرها بالتفصيل على موقع الويب وفي البرنامج بحيث يكون هناك شيء على الأقل يشير إليها من حيث تقوية النظام والإدارة الصحيحة للنظام.

وأبرز الأشياء هنا، أننا نرى توثيق الامتدادات الأمنية لنظام أسماء النطاقات. وقد نسيت ذكر ذلك لكم. فبالنسبة للخوادم الرسمية، فسوف نتوقع بالطبع أن تكون واحدة من أفضل الممارسات الريادية وهي تعزيز وتقوية مشغلي المناطق الرسمية وهي توقيع الامتدادات الأمنية لنظام أسماء النطاقات DNSSEC، وهنا في جانب وحدة حل التصديق في ذلك سوف نقوم بتشجيع - أو بالأحرى سوف نجعلها مطلبًا - لوحدات حل المصادقة أن تجري توثيقًا باستخدام الامتدادات الأمنية لنظام أسماء النطاقات DNSSEC.

ولحسن الحظ فإن هذا بالفعل هو حال الكثير من البرمجيات الموجودة على الساحة ولكننا سوف نجعل ذلك، سوف نركز عليه ونقول بأنه يتوجب عليكم إجراء عملية التوثيق باستخدام DNSSEC في هذه المرحلة الزمنية. مرة أخرى، قد يكون هذا هو الحال بالنسبة للعديد من البرمجيات. الشريحة التالية.

إذن فإن وحدات حل التصديق المشتركة التي ناقشناها هي من أنواع مزودي خدمة الإنترنت. فهم من مزودي خدمة الإنترنت أو ما يشبه ذلك. وسوف تكون لديهم متطلبات مماثلة للكثير من وحدات حل التصديق الخاصة لكن سوف يكون لديهم طيف مختلف من العملاء لأنهم سوف يتعاملون ربما مع مزيج من جوانب المحمول والكابلات والفايبر والجانب السكاني. وسوف يكون لديهم قدر من التحكيم في الوصول.

ونظرًا لأن وحدات حل التصديق هذه مشتركة فيما بين العديد من العملاء المختلفين، فإن هناك مشكلة أيضًا من حيث الخصوصية. وهناك بعض الأشياء مثل التلصص على الذاكرة المخبئية وغيرها من الأشياء التي لن نتحدث حولها الآن. لكن يجب عليك أن تتأكد عندما توفر خدمة DNS أنك تقوم بذلك بطريقة محافظة على الخصوصية، ومن ثم فإن أحد الأشياء التي نوصي بها هنا هي تمكين حل نظام أسماء النطاقات عبر بروتوكول نقل النص التشعبي الآمن DoH أو نظام أسماء النطاقات عبر بروتوكول أمان طبقة النقل أو كلاهما على خدمة وحدة حل التصديق الخاصة بك بحيث يشعر عملاؤك الذين يفضلون أكثر توجيه الاستعلامات إليك أنه يمكنهم القيام بذلك. وأيضًا عدم—ألا يغوى ولكن يشعر أن بإمكانه استخدام خدماتك وألا يضطر للتوصل إلى حل في مكان آخر سعيًا إلى وقت الاستجابة. ويمكنهم استخدام شبكتك من خلال عرض حل نظام أسماء النطاقات عبر بروتوكول نقل النص التشعبي الآمن DoH ونظام أسماء النطاقات عبر بروتوكول أمان طبقة النقل. وبإمكانهم استخدام الأنظمة الخاصة بك ويعلمون أن لديهم بالفعل علاقة أعمال معك باعتبارك موفر لخدمة الإنترنت. بعد ذلك يجب عليهم عرض حل نظام أسماء النطاقات عبر بروتوكول نقل النص التشعبي الآمن DoH ونظام أسماء النطاقات عبر بروتوكول أمان طبقة النقل. ويكون هذا الأمر مقبولاً فقط من حيث الخصوصية. وهذا أيضًا بالإضافة إلى نظام أسماء النطاقات التقليدي الحالي والمشفر والذي سيظل موجودًا لفترة من الوقت.

بالإضافة إلى توافر ومرونة خدمة DNS. وهناك عدد من التوصيات الموجودة التي نقوم بإعدادها أيضًا. وهي موجودة على موقع ويكي وسوف تتاح على موقع الويب قريبًا، وأؤكد أنها

من ممارسات الأنظمة الجيدة ومفيدة للصحة وللتقوية. ومرة أخرى، نعود إلى التوثيق باستخدام الامتدادات الأمنية لنظام أسماء النطاقات. فمن المتوقع في هذه المرحلة أن يقوم كل من يشغل وحدة حل تصديق ISP أن يجري توثيقًا باستخدام الامتدادات الأمنية لنظام أسماء النطاقات. الشريحة التالية.

بالنسبة لمشغلي وحدات حل التصديق العامة، فإننا نتحدث في الأغلب حول الوحدات الكبيرة المفتوحة، مثل Google وجميع الوحدات الأخرى. وبالطبع، فإن لديهم الطريقة الخاصة بهم في تأدية الأشياء، لكنني متأكد من أن الكثير منهم ينفذون بالفعل الكثير من أفضل الممارسات وأحد الأشياء التي نقوم بها هي وضع [يتعذر تمييز الصوت] الآن هي توثيق DNSSEC، ولحن الحظ فإن الأسماء الكبيرة تجري توثيقًا باستخدام DNSSEC واعتبارات الخصوصية، ونظام DoT وDoH. وتوفر جميع الأسماء الكبيرة إما نظام أسماء النطاقات عبر بروتوكول أمان طبقة النقل DoT أو حل نظام أسماء النطاقات عبر بروتوكول نقل النص التشعبي الآمن DoH أو كلاهما، ومن ثم من الممكن إرسال استعلاماتك على سبيل المثال، إلى Quad9 أو Cloudflare وهي 1111 واستخدام خدمة DoT أو DoH الخاصة بهم.

وهناك شيء آخر نذكره وهو اختزال استعلامات الأسماء وقد نسيت ذكر ذلك بالنسبة للآخرين، لكن اختزال استعلامات الأسماء يعني تجنب تسرب أسماء النطاقات المؤهلة كليًا بدون داع تجاه الجذر. ومن خلال تشغيل ذلك، فإنك تتأكد من أنك تكشف فقط عن جزء من اسم النطاق، لأنه سواء شئنا أم أبينا، فإن أسماء النطاقات تقوم بالكشف. فهي تكشف معلومات حول مستخدمينا وعاداتهم وما الذي يشاهدونه. ولا يكون ذلك في المعتاد للاستهلاك العام.

وينطبق نفس الشيء على وحدات حل التصديق العامة المغلقة التي توفر خدمة إما للسداد أو استنادًا إلى اتفاقية ما أو التحكم في الوصول، كما يتوجب عليهم أيضًا توفير DoT/DoH وهو ما قد يكون عليه الوضع بالفعل بالنسبة للكثير منهم.

ودائمًا ما يتم تفعيل اختزال استعلامات الأسماء حاليًا على الأغلب باعتباره ممارسة قياسية ولكننا الآن بصدد جعل ذلك -إذا جاز التعبير- مطلبًا أو نحو ذلك. وتوثيق DNSSEC، بشكل واضح. الشريحة التالية.

لا أعلم إن كان من المفترض بي أن أغطي هذا الموضوع.

آديل آكپلوغان: يمكنني تولي الأمر من هنا. شكرًا. إذن هذا الجزء من المقدم من فيل يعطينا نظرة عامة على الكيفية التي سيكون عليها هيكل أفضل الممارسات المختلفة. وأؤكد عليكم أنه يجب أن نضع في الاعتبار هدفنا هنا وهو تبسيط هذه المسألة والتركيز على العنصر الأهم، وهو الرغبة في الحصول على عدد محدد للغاية من أفضل الممارسات الواجب تنفيذها، بما لا يتجاوز هدفنا وهو 7:10 ممارسة على الإجمال لكي يتمكن الناس من تعريف أنفسهم، ولكي لا يتم الخلط بينها أكثر من ذلك.

التالي هو إعطائكم نظرة عامة بسيطة حول الطريقة التي سيتم بها تقديم وعرض وهيكلة كل ذلك عند إطلاقه. وكما قلت لكم، سوف تتم استضافته على موقع KINDNS.org والذي سيكون عبارة عن موقع ويب مخصص لذلك، ومدعوم وتحت رعاية ICANN بالأساس، حيث يمكن للأشخاص المهتمين بالانضمام إلى المبادرة بطرق مختلفة الحصول على ما يريدونه من معلومات.

إذن سوف تكون هناك جلسة تتناول الفئات المختلفة التي ذكرها فيل. أما ناحية الدعم والمشاركة فسوف تكون في النواحي التي يرغب فيها المشغلون في الانضمام إلى المبادرة ودعمها ويمكنهم الانضمام إما في صورة راعي أو عضو أو مشغل نطاق أو سفير للمبادرة.

وبعد ذلك سوف نجري جلسة أدوات يمكن للمشغل فيها إجراء تقييم ذاتي لنفسه. وما زلنا نناقش وننظر في الكيفية التي ستكون عليها أداة التقييم الذاتي تلك. وما نريده، هو أننا نريد أن يكون هذا الأمر سهلاً وبسيطًا ومباشرًا للغاية لأننا لا نفرض هذا الأمر ولا نجعله إلزاميًا. فهذه مشاركة تطوعية، ومن ثم يجب على الناس المشاركة من طرفهم في الالتزام بتنفيذ هذه الممارسات المثلى عمومًا.

إذن فأداة التقييم الذاتي أيضًا سوف تكون مستندة في الأغلب على الالتزام الذاتي للناس هنا في تنفيذ بعض من تلك الممارسات والرد على تلك الأسئلة المطروحة على سبيل المثال.

وسوف تكون لدينا لوحة إعلانات. سوف نقوم بتطوير لوحة إعلانات من شأنها توفير بعض المعلومات لكم. وكما ذكرت آنفًا، أن تكون لنا القدرة أيضًا على تعقب بعض المعرّفات التي سيقع عليها اختيارنا للسماح لنا برؤية كيفية تأثير ذلك على المشهد العام عمومًا. وبعد ذلك سوف يكون

لدينا أيضًا الإرشادات التوجيهية حول كيفية تنفيذ أفضل الممارسات أو تقديم المزيد من التفاصيل والمزيد من المعلومات حول أي من الممارسات المثلى أو الاعتبارات.

على سبيل المثال، إذا ما ألقينا نظرة فاحصة على الشريحة التي ذكر فيها فيليب كل ما يتعلق بتقويم الجوهر أو أمن النظام وكل تلك الأشياء، والتي لن تكون جزءًا من أفضل الممارسات الجوهرية فسوف يتم تسليط الضوء عليها في الإرشادات التوجيهية، على سبيل المثال، حيث يمكن للناس الاطلاع عليها والنظر فيها. لكنها ليست جزءًا من جوهر ما نريد القيام به. وبعد ذلك معنا المدونة والفعاليات وكل الأشياء الأخرى ذات الصلة بذلك.

ومن ثم، فإننا نعمل باتجاه ذلك، ونقوم بالتلخيص، وتحديد أكثر الممارسات المثلى حيوية، كما أننا بدأنا في تطوير ووضع بعض الإرشادات التوجيهية. وقد أطلقنا مؤخرًا دليلاً إرشاديًا لتوقيع الامتدادات الأمنية لنظام أسماء النطاقات DNSSEC في واحدة من مستندات [مكتب المسئول الفني الأول]. وسوف تتم الإشارة والرجوع إلى هذا النوع من المستندات بشكل واضح في مبادرة تبادل المعرفة وتجسيد معايير نظام أسماء النطاقات وأمن التسمية والعديد من الإرشادات التوجيهية الأخرى سوف يتم إطلاقها قريبًا. الشريحة التالية، من فضلك.

لدينا الآن مقاول معنا في العمل لمساعدتنا على تصميم وتطوير موقع ويب جديد، ربما سيكون مظهره وتصميمه مشابهًا لهذا إلى حد ما، لكننا ما زلنا في المرحلة المبكرة للغاية من [مساعدتهم] على التوصل إلى التصميم النهائي والشكل النهائي لذلك. لكن في حقيقة الأمر سوف يكون ذلك المحصلة التالية لهذا المشروع عمومًا. الشريحة التالية.

إذن فقد توجب علينا تعديل إطارنا الزمني قليلاً منذ المرة الأخيرة التي أجرينا فيها هذا العرض التقديمي لأسباب متنوعة، لكن هدفنا الآن يتمثل في أن تكون لنا القدرة على إطلاق هذا الموقع بنهاية الربع الأول من عام 2022 وسوف ينتهي تقريبًا بنهاية شهر مارس/آذار.

وربما لن نحصل على جميع وظائف موقع الويب لكننا سوف نطلق الوظيفة الأكثر أهمية والتي يمكن أن تتيح لنا البدء في تشغيل هذا، والبدء في الطرح ومشاهدة المشغلين في هذا الأمر.

وسوف نحيط المجتمع علمًا بالإضافة إلى القائمة البريدية على طول الطريق. وأنا أوصيكم بالانضمام إلى القائمة البريدية، إذن أردتم ذلك. فهي قائمة بريدية مفتوحة. ويمكن لأي أحد الانضمام وتزويدنا بالتعقيبات والآراء والإسهام في مناقشة هذه المسألة.

وفي نفس الوقت أيضًا، فقد أنشأنا صفحة ويكي ننشر عليها غالبية الأشياء التي نعمل عليها في الوقت الحالي ونتخذها مستودعًا مؤقتًا. وسوف تنتقل تلك الصفحات إلى موقع الويب الرسمي عندما نقوم [بإضافتها].

وأعتقد أن هذه هي الشريحة الأخيرة. نعم. شكراً لكم جميعاً على حسن انتباهكم. لذا نود أن نستمع إلى آرائكم وأسئلتكم وتعليقاتكم ومقترحاتكم. فهذا هو الهدف من هذه الجلسة. شكرًا.

كنغا كوالزيك: لدينا سؤال في مربع الأسئلة والأجوبة. آديل، هل تريد مني قراءته بصوت عالٍ؟

آديل آكپلوغان: نعم من فضلك.

كنغا كوالزيك: إذن، لدينا سؤال من سيفاسوبرامانيان. "هل ستقوم مبادرة تبادل المعرفة وتجسيد معايير نظام أسماء النطاقات وأمن التسمية بتطوير التزم مشترك، بعدم إلزام المستخدمين بوحدة حل تصديق واحدة ولكن الإبقاء على وحدات حل مصادقة متعددة يمكن للجميع استخدامها؟ هل سيناريو [قاس] وغير دقيق وربما مستبعد أيضًا. هل يؤدي ذلك [يتعذر تمييز الصوت] إلى قيام الجامعة بحجب الطلاب عن استخدام وحدات حل تصديق خارجية أو إصرار العمدة على عدم استخدام كل من في المدينة لوحدة حل تصديق خاصة بمدينة أخرى؟ هذا السيناريو وغيره من الالتزامات المشتركة ذات الصلة بعيدة كل البعد عن مشاركة أفضل الممارسات".

آديل آكپلوغان: شكرًا. هذا السيناريو شيق للغاية. الأسئلة متصلة وذات صلة وثيقة بجانب المسجلين في هذا الاجتماع، أي جزء المستخدمين. ويرتبط أكثر بالسياسات لأن هذه قرارات تخص السياسة عندما يطلب شخص ما من عميله أو المستخدم أو من المجتمع أو من المواطن استخدام مشغل محدد أو خدمة بعينها. والشق الخاص بالسياسات غير مشمول هنا بشكل أو بآخر لأن لدينا قدر ضئيل للغاية من الرقابة والتحكم في تلك الأشياء.

ومن منظور المسجلين وعمليات التشغيل، بالطبع يمكنكم استخدام العديد من وحدات حل التصديق في الإعداد الخاص بك وهذا بشكل عام يعد ممارسة مثلى لإدارة الشبكات، وممارسة مثلى عامة لتوفير الخدمات والمواطنة والوفرة في خدمة DNS عمومًا. لكننا لم نركز هذا الأمر على تلك الناحية على وجه الخصوص لأنها تتعلق بشكل أكثر بالمسجل وبجانب أفضل ممارسات موفر خدمة الإنترنت، وليس جوهر عمليات نظام أسماء النطاقات DNSOP في حد ذاتها.

كنغا كوالزيك: ليس لدينا أي أسئلة أخرى. أرجو من الجميع إن أراد أحد طرح سؤال أن يرفع يده وسوف نقوم بكتم صوت الميكروفون لديه وإعطاءه فرصة التحد أو كتابة سؤاله في مربع الأسئلة والأجوبة وسوف أقرأه على مسامع الجميع.

آديل آكپلوغان: أود أن أستمع من المشاركين حول جانب واحد في هذا الموضوع. وقد أتى فيل على ذكره. أعتقد أنه ذلك الجانب في الشريحة التي تتحدث حول وحدة حل التصديق العامة التي نؤكد فيها على اعتبارات الخصوصية والتي تعد جانبًا قمنا بمناقشته كثيرًا على المستوى الداخلي.

وكما تعلمون جميعًا، فإن مسألة DoH and DoT كانت في البداية خلافية للغاية، وأثارت الكثير من المخاوف في البداية، لكن هناك الكثير والكثير من مشغلي وحدات حل التصديق ينفذون ذلك وهي من الممارسات المثلى بالنسبة للخصوصية عمومًا.

السؤال هو ما مقدار اعتبارات الخصوصية تلك الذي يجب أن يكون جزءًا من مبادرة تبادل المعرفة وتجسيد معايير نظام أسماء النطاقات وأمن التسمية؟ فعندما ننظر في وثائق أفضل الممارسات الاعتيادية، حتى العام الماضي، في غالبيتها ... نجد أنه اعتبارات الخصوصية لم يتم تسليط ما يكفي من الضوء عليها. لكن على مدار الأعوام القليلة الماضية، باتت الخصوصية ضمن أهم الاعتبارات بالنسبة للمستخدمين على الإنترنت.

ومن ثم شعرنا بأن الخصوصية يجب أن توضع في اعتبارات مبادرة تبادل المعرفة وتجسيد معايير نظام أسماء النطاقات وأمن التسمية عمومًا. كما أن اختزال استعلامات الأسماء يمس

الجميع، من منظور وحدة حل التصديق ووجوب قيامهم بذلك، فهي مباشرة وواضحة، وهي غالبية البرمجيات ومن ثم لا أعتقد أن هناك خلاف في ذلك. أنا لا أي منها.

وعلى الرغم من ذلك، فيما يخص DoT أو DoH، نجد من يبدي في بعض الأحيان تعجبه. "يا إلهي، هل سنتناول هذه المسألة؟ هل ستذكرون ذلك في بند أفضل الممارسات أم لا؟" وفيما يخص القائمة البريدية، لم يكن هناك دليل ملموس [يتعذر تمييز الصوت] حتى الآن حول هذين الأمرين، وعلى وجه الخصوص DoT، لكنني أود الاستماع إلى ما قد يكون للناس من آراء حول الخصوصية، من منظور اعتبارات الخصوصية وDoT وDoH. هناك يد مرفوعة. لقد رفع أولريخ يده. هل يمكن لأي أحدى أن يفتح له الميكروفون بحيث يمكنه التحدث؟

أولريخ فيزر: مرحباً. أنا أولريخ. نعم. شكرًا لك آديل على إتاحة فرصة التحدث لي هنا. أردت القول بأنني أعتقد ... أن نظام أسماء النطاقات عبر بروتوكول أمان طبقة النقل DoT يحل بعضًا من اعتبارات الخصوصية، لأنه وبشكل واضح لا يتيح للناس [يتعذر تمييز الصوت] الاستماع إلى طلبك، لكن ما يزال عليك وضع الكثير من الثقة في المشغل الذي تتعامل معه. ولا يمكن حل ذلك بشكل واضح إلا من خلال تصميم Oblivious DNS لكنني لا أعتقد أن تصميم Oblivious DNS جاهز الآن لأن يكون على مقربة من أفضل الممارسات.

آديل آكپلوغان: أتفق معك في الرأي.

أولريخ فيزر: لكنني أعتقد أن هذا من الأشياء التي ربما يجب ذكرها، وهي أن نظام أسماء النطاقات عبر بروتوكول أمان طبقة النقل DoT يحل بعضًا من مشكلات الخصوصية لكنه غير قادر على حل كل شيء.

آديل آكپلوغان: شكرًا. هذا تعقيب رائع من منظور المشغلين. لقد ذكرت شيئًا هامًا ولافتًا أيضًا. علاقة الثقة القائمة بالفعل إلى حد ما بين مستخدم وحدة حل التصديق وموفر الخدمة. على سبيل المثال، في سياق مزود خدمة الإنترنت، من الواضح أن هناك اتفاقية خدمة. كما أن هناك شكل من أشكال القيود، وهو ما قد يجعل اعتبارات الخصوصية تنتقل بمعنى أو بآخر أو إذا كان [يتعذر تمييز الصوت] حيث تكون لديك سياسة تجبرك على استخدام وحدة حل التصديق الخاصة بشركتهم فمن المتحمل أن يؤدي ذلك إلى التقليل من جانب الخصوصية قليلاً لأنك بكل الأحوال تستدام شبكة الشركة، ومن ثم يتوجب عليك الالتزام ببعض السياسات.

لكن عندما تكون في الخلاء دون أي قيود، ربما يكون هذا هو المكان الذي تصبح فيه الخصوصية أكثر أهمية وهذا هو السبب في أننا نضع اعتبارات الخصوصية إلى حد ما—نحاول وضع اعتبارات الخصوصية بمزيد من التركيز في الفئة التي تغطي الجانب المفتوح والعام من وحدات حل المصادقة حيث يمكن لأي أحد أن يقرر استخدام أي وحدة حل تصديق وهذا هو المكان الذي قد يكون فيه الجميع أكثر اهتمامًا بالخصوصية وما يقومون بتوقيعه لوحدة حل التصديق.

هل هناك أي أحد لديه ما يريد طرحه في جانب وحدة حل التصديق أو فيما يخص [يتعذر تمييز الصوت] بالطبع أيضًا فيما يخص مبادرة تبادل المعرفة وتجسيد معايير نظام أسماء النطاقات وأمن التسمية وأفضل الممارسات التي نستعرضها؟

حسنًا. إذا لم تكن هناك أية أسئلة أو تعليقات أخرى، فهذا يعني أننا في ... أرى أننا في الاتجاه الصحيح. أتوجه بالشكر إلى كل من انضم إلى القائمة البريدية وقدم إسهامًا حتى الآن في المبادرة. أعتقد أن هناك سؤال واحد. نعم، هناك سؤال واحد في مربع الأسئلة. لقد فاتني ذلك. هل يمكنك قراءته؟

كنغا كوالزيك: نعم. هل القياس جزء من تصميم مبادرة تبادل المعرفة وتجسيد معايير نظام أسماء النطاقات وأمن التسمية، شكل من أشكال القياس تكون فيه للمجتمع طرق يستخدم في تقييم بيانات وحدة حل التصديق التي تستخدمها وحدات حل التصديق المتنوعة وطريقة للمقارنة؟ هل القياس جزء من تصميم مبادرة تبادل المعرفة وتجسيد معايير نظام أسماء النطاقات وأمن التسمية؟

آديل آكپلوغان: حسنًا، كما ذكرت لكم فسوف نحدد مؤشرًا يتيح لنا إمكانية التعرف على كيفية تأثير ذلك على بعض جوانب الأمن في عمليات نظام أسماء النطاقات على الإجمال. لم يتم إلى الآن تحديد ما ستكون عليه تلك المؤشرات تحديدًا واضحًا. وربما أيضًا نقوم بمشاركة بعض من هذه المعرّفات من مبادرات ICANN الأخرى، مثل [مؤشرات جودة تقنيات المعرّفات] على سبيل المثال أو غيرها من المؤشرات، أي المبادرات الموجودة بالفعل.

لكن في السؤال الحالي، ثمة ذكر لتقييم أي من بيانات وحدة حل التصديق. لا أعلم أي أنواع البيانات التي يجري قياسها هنا وما صلة ذلك بهذه الحالة الخاصة.

وفي المعتاد، ومن منظورنا نحن، عندما نقوم بقياس هذا النوع من الأشياء، فإننا نحاول قياس ما يمكننا قياسه من منظورنا نحن، وليس محاولة الوصول إلى بيانات خاصة ليس لنا سيطرة أو رقابة عليها. وربما أيضًا نقوم بقياس تلك الأشياء طبقًا لذلك وفقط فيما يتصل بأفضل الممارسات الموجودة لدينا في [يتعذر تمييز الصوت] ربما يمكننا القول بأن، عدد وحدات حل التصديق ذات اعتبارات الخصوصية [يتعذر تمييز الصوت] على طول هذا الطريق عبر مدار الشهر الفائت، العام الفائت أو نحو ذلك من خلال قياس وحدات حل التصديق تلك ذات نظام DoT أو DoH أو اختزال استعلامات الأسماء النشطة. هذه إحدى الطرق التي يمكننا من خلالها قياس ذلك مباشرة.

لكنني لا أفهم ما تقصده بتقييم بيانات وحدة حل التصديق، لأننا عندما نبدأ في التحدث حول تقييم بيانات وحدة حل التصديق، فإن هذا يعطينا وجهة نظر مختلفة تمامًا حيال الأمر. وسوف نقوم بقياس ما يمكننا قياسه بشكل عام، ولكن فقط فيما يتعلق بأفضل الممارسات التي كنا في السابق [نلتزم بها].

بالإضافة إلى ذلك، فإننا نرغب في المشاركة والحصول على أكبر قدر ممكن من وحدات حل التصديق للانضمام إلى المبادرة والالتزام بأفضل الممارسات تلك. وإذا حدث خلال مسيرة هذا الأمر أن نجحنا في الحصول على طريقة للتعاون والعمل مع بعض وحدات حل التصديق للقيام بمزيد من القياس المتطور والدراسة المتطورة حول ما يرونه، فيمكن بالطبع إضافة ذلك إلى المبادرة.

لكن مرة أخرى، سوف نجعل هذا الأمر واضحًا ومباشرًا قدر الإمكان، ومن ثم فإن ما نقوم بطرحه لا يمثل أو يشكل أي تضاد لكل من المستخدمين وأيضًا لمن سيقومون [يتعذر تمييز الصوت] نتيجة المبادرة.

حسنًا. إن القائمة البريدية مفتوحة. فلا تترددوا في الانضمام ويمكننا مواصلة بعض من هذه المناقشات هناك. ويمكنكم طرح الاعتبارات أو الأسئلة الأخرى التي لديكم هناك أو يمكنكم التوصل معنا مباشرة في مكتب المسئول الفني الأول. ويمكنكم مراسلتنا مباشرة على البريد OCTO@ICANN.org أيضًا إن كان لديكم أسئلة مباشرة.

أرى سؤالاً واحدًا من ديزيري. شكرًا لك، ديزيري. نعم. وكما ذكرت لكم، هناك مراسلة ومكون خاص بالتواصل والتوعية لهذا الأمر تم تسليط الضوء عليه إلى حد كبير أيضًا. وبالطبع فإننا نعم مع المجتمع بشكل عام. ولكن هذا هو السبب في أن لدينا برنامج للسفراء مخبأ في مكان ما هناك حيث سنعمل مع المجتمع من أجل تعزيز وتقوية هذا الأمر. لكن ICANN أيضًا سوف تخصص بعض الموارد من أجل إفشاء وتعزيز المبادرة عند الإعلان عن إطلاقها. وبالطريق فإن النجاح سوف يعتمد بشكل كبير على التعزيز والتقوية وربما أيضًا على كيفية تيسير الوصول إلى هذا الأمر وسهولة استيعاب المجتمع له.

شكرًا لكم جميعًا على تشريفكم لنا بحضوركم هذه الجلسة. لم يتبق لدينا إلى تسع دقائق من الوقت المخصص لنا لهذه الجلسة. ولا أرى أن هناك أية أسئلة أخرى، لكنني سعيد للغاية بمقابلتكم جميعًا في القائمة البريدية دون اتصال من أجل مناقشة هذه القضية. هل هناك أي شيء آخر، كينغا، يجب علينا الحديث حوله؟ وإلا فالكلمة إليك مرة أخرى.

كنغا كوالزيك: لا، فقد أجبنا عن جميع الأسئلة. شكرًا لكم جميعًا. سوف يتم نشر العرض التقديمي أيضًا على موقع الويب على موقع اجتماع ICANN73 على الويب في غضون يومين ربما. شكرًا.

آديل آكيلوغان: شكرًا لك، كينغا. أشكرك، ستيفن. وشكرًا لك، فيل، أيضًا. إلى اللقاء، جميعًا.

فيل رينو: شكرًا.

[نهاية التدوين النصي]