اجتماع ICANN76 | برنامج زمالة ICANN – CF:تعريف بمكتب المسئول الفني الأول في ICANN ومبادرة تبادل المعرفة ومعايير التمثيل لنظام أسماء النطاقات وأمن التسمية KINDNS
الأحد الموافق 12 مارس/آذار 2023 – في تمام الساعة 10:30 إلى 12:00 بتوقيت كانكون

سيرانوش فاردانيان: أهلاً ومرحبًا بكم جميعًا في اليوم الثاني من اجتماع ICANN76. أتمنى أن تكونوا قد استمتعتم جميعًا بيوم أمس. أنا سيرانوش فاردانيان، وأرحب بكم جميعًا في هذه الجلسة مع فريقنا الفني ومع فريق هيئة الإنترنت للأرقام المخصصة IANA. وسوف يطلعونكم على المزيد حول كل هذه الاختصارات.

لكن قبل ذلك، إليكم إعلان قصير. سوف أكون أنا مدير المشاركة عن بعد معكم لهذه الجلسة، وسوف يتم تسجيل هذه الجلسة وسوف تخضع لمعايير ICANN للسلوك المتوقع.

وسوف تُقرأ الأسئلة والتعليقات المرسلة في الدردشة خلال هذه الجلسة على مسامع الجميع إذا وُضعت بالشكل السليم المُشار إليه في مربع الدردشة. إذا أردتم التحدث أثناء هذه الجلسة, فيرجى رفع اليد في برنامج زووم، وعند مناداة أسمائكم سوف يقوم المشاركون عبر الإنترنت بإلغاء كتم صوت ميكروفوناتهم في برنامج زووم. وسوف يستخدم المشاركون الحاضرون بشخصهم ميكروفوناتهم الفعلية. ولدينا اثنان من الميكروفونات المتنقلة هناك. مراعاةً للمشاركين الآخرين، يرجى ذكر اسمك للتدوين في السجل والتحدث بوتيرة معقولة.

ولدينا ترجمة فورية بلغات الأمم المتحدة الست وأنا أهيب بالجميع قبل الجلوس الحصول على سماعات الرأس والاستعانة بالترجمة الفورية. فلدينا فريق ترجمة فورية رائع.

وبهذا، أود أن أعرفكم على الحاضرين معنا اليوم وأود البدء بالمسئول الفني الأول، جون كرين، الحاضر هنا مع الفريق، وديفيد وكيم ديفيز، الذي سيعرفكم على هيئة الإنترنت للأرقام المخصصة IANA ويحدثكم حولها. لكننا سوف نبدأ مع جون. جون، الكلمة لك.

جون كرين: شكرًا جزيلاً. من الرائع رؤيتكم جميعًا هنا. كما تعلم سيرانوش، فإن الزملاء وبرنامج NextGen هي المجموعات المفضلة لدي في ICANN لأنكم جميعًا من الوجوه الجديدة ذات الأفكار الغضة

وما إلى ذلك، لذلك دائمًا ما يسرني الحضور هنا. معكم جون كرين. أنا نائب الرئيسي الأول والمسئول الفني الأول في ICANN. وقد التحقت بـ ICANN منذ عدة عقود أو أكثر إلى الآن. لقد مرت فترة من الوقت. وأنا جزء من الأثاث الكائن هنا، إن جاز التعبير.

كما أنني أدير مجموعة يطلق عليها اسم IROS. وأنا أعلم أنكم لا تسمعون الكثر من الأخبار عنها في الخارج. فهي أحد أشكال التميز الداخلي الذي لدينا هنا. ونحن المجموعة المعنية بالاختصارات. نحن نحب الاختصارات. ومن ثم فإن IROS هي المعرّف (فهي تتعلق بأسماء النطاقات وعناوين IP وجميع المعرّفات [الموجودة]) والبحث والعمليات والأمن. والحرف الأول "I" هو الأهم. فكل ما يهمنا في ذلك هو المعرفات وما يدور في هذا الشأن.

ويمكنكم تقسيم هذا الأمر إلى ثلاثة أنواع من الأنماط المتباينة. معنا مجموعة يطلق عليها اسم IANA (هيئة الإنترنت للأرقام المخصصة)، والتي تدار بمعرفة السيد المحترم إلى يساري، كيم ديفيز. وبعد ذلك معنا مجموعة ينصب اهتمامها أكثر على المشاركة في المسائل الفنية، وتدار بمعرفة شخص محترم وصديق عزيز يطلق عليه آديل، لكن معنا ديفيد على يميني هنا. بعد ذلك الكثير من الأبحاث. وهناك اثنان من المديرين التابعين لي يعملان على ذلك. أرى أحدهم تعلوه حمرة الخجل ويختبئ بين مجتمع الحاضرين. قل مرحبًا، سامانا. لم لا ... يمكنك المجيء والانضمام إلينا إن شئت ذلك. ولا أرى مات، لكنني أعلم—ها هو مات. مات يمكنه المجيء والانضمام إلينا أيضًا، إن شئتم ذلك، ويمكنه التزام الخجل والبقاء هناك. الأمر عائد إليكم.

والآن هذه هي الأشياء التي نقوم به. فنحن نجري أبحاثًا حول جميع الأشياء التي تؤثر على المعرِّفات. وتقوم سلسلة هيئة الإنترنت للأرقام المخصصة بإدارة الكثير من هذه المعرِّفات من منظور تشغيلي. ثم ننطلق بعد ذلك ونتحدث حول تلك الأشياء.

ومن ثم فإنني لا أود تقضية الوقت في التبشير لديكم، ومن ثم سوف أعطي المزيد من القوت لبعض من هؤلاء السادة من أجل الحديث حول الأشياء التي يعملون عليها. وسوف أبدأ فيما نعتبره الشيء الأكثر أهمية الذي تقوم به ICANN لأنكم هنا في اجتماع خاص بالسياسات، لكن السياسات هامة فقط إذا كان بإمكانكم فعليًا وضعها في موضعها الصحيح والتمكن من إدارة تلك المعرّفات فعليًا. ومن ثم سوف أحيل الكلمة إلى كيم، إن شئتم. لم لا تخبرنا بالقليل من المعلومات حول دور هيئة الإنترنت للأرقام المخصصة IANA؟

كيم ديفيز: إذن سوف أوجز في كلمتي لأن لدي بالفعل عرض تقديمي لكنني سوف أعرضه على الفور. من المفترض أن يكون دور هيئة الإنترنت للأرقام المخصصة IANA متمثلاً في كونها دارًا للمقاصة المحورية، ومستودع للسجلات من أجل جميع المعرّفات التي نستخدمها على الإنترنت. أعتقد أن الغالبية هنا يعرفون كل ما يخص أسماء النطاقات. فهم غالبًا ما ينظر إليهم بشكل عام عندما نتحدث حول معرّفات الإنترنت، لكنهم ليسوا الوحيدين بأي حال من الأحوال. وربما تكون عناوين IP هي أيضًا معروفة بالنسبة لكم، لكن هناك فعليًا آلاف المعرّفات المستخدمة من أجل تمكين الاتصالات اليومية عبر الإنترنت والتي قد لا تكونوا على دراية بها. فلكي يعمل الإنترنت، يجب أن يكون هناك مكان مركزي يتم فيه تخصيص تلك المعرّفات مركزيًا بحيث يتم ذلك بشكل متسق في جميع أنحاء العالم. وهذا يقع في صميم ما تقوم به وظائف IANA في حقيقة الأمر. ومن ثم سوف نتطرق إلى هذه النقطة بعد قليل، لكن هذا باختصار ما نقوم به.

جون كرين: حسنًا. أما حرف "R" فيرمز إلى الأبحاث. إذن سامانا أو مات، لم لا تحدثنا قليلاً حول أساسيات ما تقوم به المجموعات الخاصة بكما.

ساماتا تاج علي: أنا ساماتا تاج علي زادة خوب، وأنا أقود مجموعة الأبحاث المعنية بالأمن والاستقرار والمرونة (SSR) داخل مكتب المسؤول الفني الأول CTO. أي الموضوعات الأكثر ارتباطًا بشكل غير مباشر أو بشكل مباشر بأمن نظام أسماء النطاقات. وربما تكون بعض الموضوعات التي تسمعون بها كثيرًا في اجتماعات ICANN، ألا وهي انتهاك نظام أسماء النطاقات DNS ولكن أيضًا عمليات تكوين وإعدادات أمن نظام أسماء النطاقات، وجميع الأشياء غير المباشرة التي تؤثر على الأسماء والتي تؤثر أيضًا على الانتهاك—أشياء من قبيل التصيُّد والبرمجيات الضارة والتحكم والسيطرة وأمن الويب وأمن البروتوكولات، إلخ.

والآن سأنقل الكلمة إلى مات.

مات لارسون: أنا مات لارسون. أنا أيضًا أدير فريقًا للبحث. وفي بعض الأحيان نقوم بأعمال الأمن، ولكن لا نركز دائمًا على أعمال الأمن، على النحو الذي يقوم به فريق ساماتا. ونؤدي الكثير من العمل.

ولدينا بعض مجموعات البيانات الكبيرة التي نعمل عليها. وقد أسعدنا الحظ بإمكانية الاطلاع على مرور البيانات إلى خادم الجذر المدار بمعرفة ICANN. ومن ثم فإننا نجري بحثًا استنادًا إلى ذلك. ونجري أيضًا أبحاثًا استنادًا فقط إلى محتويات نظام أسماء النطاقات. كما أن لدينا إمكانية الوصول إلى جميع ملفات منطقة نطاقات gTLD وبعض ملفات منطقة نطاقات ccTLD. إذن هذه هي مجموعات البيانات الثرية للغاية التي نعمل عليها أيضًا. كما أننا نشطون في ناحية المعايير، وعلى وجه الخصوص فريق عمل هندسة الإنترنت. ومن ثم فإن نجري أيضًا عمليات توضيح للبروتوكولات والتعزيزات والمستندات المرتبطة بالتشغيل أيضًا.

جون كرين: ديفيد، لم لا تتحدث قليلاً حول أعمال المشاركة؟

ديفيد هوبرمان: بالتأكيد، مرحبًا. طاب صباحكم جميعًا. أنا ديفيد هوبرمان، وأعمل في هذا القسم الذي يطلق عليه اسم المشاركة الفنية. ونحن عبارة عن فريق مكون بالأساس من مهندسين من جميع أنحاء العالم يعملون مع كل من المجتمع الفني والمجتمع غير الفني من أجل بناء قدرات جيدة وبناء مهارات حول الامتدادات الأمنية لنظام أسماء النطاقات DNSSEC، وحول التوجيه الآمن للبيانات وزاوية البنية التحية العامة الأساسية RPKI مع سجلات الإنترنت الإقليمية. ونحن نعمل المشاركة، وعلى وجه الخصوص مع المجتمعات غير الفنية، حول الموضوعات ذات الصلة بـICANN من أجل ضمان حصول الجميع على فهم جيد وقوي بالأعمال الهندسية التي تقوم عليها البنية التحتية للإنترنت والطريقة التي تبنى بها الإنترنت. كما أننا نعقد شراكة مع العديد من الأصدقاء والزملاء هنا في ICANN ونبذل جهودًا داخل الحكومات والمجتمعات غير الفنية من أجل ضمان اتفاق الجميع على الطريقة التي تعمل بها الإنترنت.

جون كرين: لقد كانت هذه نظرة عامة رائعة.

وسوف أطلب منكم المرور على الأسئلة في عجالة لأنكم قد استمعتم بما فيه الكفاية حول هذا الأمر، ولكن قبل ذلك، هل يمكن لفريق مجموعة المعرفات والبحث والعمليات والأمن في القاعدة التكرم بالوقوف بحيث يعرف الحاضرون مع من يتعاملون ويختارون؟

حسنًا. إذن هناك مجموعة منا هنا معنا في اجتماع ICANN. والآن، فإن فريق العمل أكثر من ذلك، لكننا نحضر فريقًا صغيرًا إلى اجتماع ICANN بحيث يمكننا التفاعل مع المجتمع والقيام بالعمل هنا. لذلك من المهم الاستماع منكم هنا.

ومن ثم سوف أحيل الكلمة مرة أخرى إلى زميلي هنا، وسوف أتأكد مما إن كان هناك أي أسئلة.

سيرانوش فاردانيان: شكرًا لك، جون. الجلسة مقررة في الأساس من أجل الزملاء ومن أجل المشاركين في برنامج NextGen للجيل التالي، ومن ثم فإنني أوصيكم جميعًا بالمشاركة بنشاط بطرق الأسئلة لأن هذه فرصة فريدة لكم جميعًا. والعديد منكم ليسوا من المتخصصين في المجال الفني، لكن من المهم للغاية فهم الطريقة وتكوين وجهة نظر فنية حول الطريقة التي تعمل بها ICANN. لذلك أرجو منكم جميعًا عدم التردد والخجل. وقد أخبرتكم خلال الجلسة الأولى، بأنه لا يوجد ما يسمى بالأسئلة الغبية على الإطلاق. لذا تفضلوا بطرح الأسئلة، ويمكننا البدء من الآن. أيًا ما يكون مهمًا بالنسبة لكم. ولدينا ميكروفونات. فهلا طلبنا وضع اثنين من الميكروفونات هنا. أعتقد أنهم لدينا [بالفعل]. إذن مكن لأي شخص رفع يده. نعم، الميكروفونات في الطريق إليكم. أمهلونا قليلاً فقط.

نعم، من فضلك. هنا. هل يمكنك تناول الميكروفون؟ وبعد ذلك سوف يبدأ الأمر هنا.

نيكولاس، سنعود إليك، نعم. شكرًا.

هاريش تشوداري: مرحبًا بكم جميعًا. أنا هاريش تشوداري، زميل ICANN. إذن أنا طالب في مجال الأبحاث في جامعة العلوم الشرعية الوطنية بالهند، وأبحاثي تدور حول أمن نظام أسماء النطاقات. وسؤالي موجه إلى فريق البحث، كيف يمكنني المشاركة؟ لأنني أعمل على وجه الخصوص على أمن نطاق ccTLD الخاص بالهند والمقاييس ذات الصلة به. إذن كيف يمكنني الإسهام في العمل؟ كيف يمكنني تعلم تكنولوجيا جديدة من الفريق بحيث يساعد ذلك في كلا الجانبين؟ شكرًا.

جون كرين: ساماناً، هلا أجبت على هذا؟

ساماتا تاج علي: نعم. شكرًا لك، جون. شكرًا على السؤال. سعيدة بمشاركتكم هنا في القاعة. في الحقيقة، أنا أعرف على وجه اليقين ... لا أدري إن كنتم أيها السادة على دراية بمشروع الإبلاغ عن نشاط انتهاك النطاق DAAR في ICANN القائم منذ ما يقرب من أربعة أعوام إلى الآن. وهو يطلق عليه اسم أداة الإبلاغ عن إساءة استخدام النطاقات. ونطاق الهند جزء من ذلك المشروع. ومن ثم فإننا داخلون في تعاون بشكل ما بالفعل مع نطاق الهند. وأود أن أستمع منكم حول ماهية موضوعات الأمن التي تعملون عليها إن كان بإمكانكم تسهيل الأمر، وإن كان بإمكاننا العمل معًا، وإن كان بإمكاننا توفير البيانات المفيدة أو الحديث حول ذلك. أشر إلى الاتجاهات الصحيحة إن احتجت إلى ذلك. لكننا نقوم بالكثير من الأعمال التي تدور حول أمن نطاق المستوى الأعلى، ومن ثم يجب أن تكون هناك جوانب يمكننا فيها توجيهكم فيها أو توفير المساعدة لكم بشكل أو بآخر.

جون كرين: نعم. وإذا سمحتم لي، فإننا ننشر أيضًا الكثير من المستندات فيم يطلق عليه اسم سلسلة مكتب المسئول الفني الأول. وإذا ما رأيتم إحداها ورأيتم أنها شيقة وكنتم تعتقدون أنها جيدة ورأيتم أنها مريعة—آمل ألا تكون كذلك—فاكتبوا لنا. تعليق. برجاء أخذ ما يكفيكم من الوقت للانتقال إلى ساماتا والتحدث إليها أو إلى أي من أعضاء الفريق هنا. فنحن دائمًا ما نبحث عن أشخاص من أجل التعاون معهم ومعرفة ما إن كنا نقوم بالأبحاث الصحيحة أو ما إن كانت هناك طرق يمكننا من خلالها تحسين مستوى أبحاثنا.

سيرانوش فاردانيان: شكرًا. نيكولاس، هلا تفضلت؟ أنت التالي.

نيكولاس فيوماريلي: مرحبًا بفريق مكتب المسئول الفني الأول في ICANN. معي هنا موضوع أمن توجيه مسار البيانات وهو ليس جزءً من مهمة ورسالة ICANN أو أهدافها، لكنكم ذكرتم مؤخرًا البنية التحية العامة الأساسية وأهميتها على أمن توجيه مسار البيانات. إذن كيف يمكنكم توضيح طريقة ملاءمة أمن توجيه مسار البيانات مع أعمال ICANN، إن كان الأمر كذلك؟

إضافة إلى ذلك، إذا كان أمن توجيه مسار البيانات جزء فعلي من أبحاث ICANN، فإنني أشعر بالفضول تجاه مرونة ومتانة البنية التحتية للشركات الكبرى والتطبيقات المشهورة. على سبيل المثال، منذ بضع سنين، كانت هناك حادثة تورطت فيها شركة Meta (فيسبوك سابقًا) وانطوت على فشل نظام أسماء النطاقات DNS وخطة استمرارية العمل BCP. هل يمكنكم العثور على وجهات نظر حول كيفية معالجة شركات مثل شركة Meta أمن توجيه مسار البيانات وما الخطوات التي يتخذونها من أجل ضمان مرونة ومتانة البنية التحتية؟ نشكركم على ما بذلتموه من وقت وما أبديتموه من وجهات نظر.

جون كرين: حسنًا، لقد كانت هذه أسئلة كثيرة. سوف أحاول تقسم البعض منها، وسوف أبدأ بالسؤال الأول البسيط، ألا وهو هل توجيه مسار البيانات ضمن اختصاص ICANN؟ إذن ICANN لا يعنيها نظام أسماء النطاقات. بل إن اهتمامها منصب على المعرّفات. وإذا ما اعتبرتم أن التوجيه يخص عناوين IP كما أن حل الأسماء يخص نظام أسماء النطاقات، فمن الواضح أن لدينا اهتمام بهذا الأمر.

والآن، فعندما نتعامل مع الأشياء التي تدور حول نظام أسماء النطاقات، فإن شركائنا—لأن ICANN جزء من المجتمع—يميلون لأن يكونوا من السجلات وأمناء السجلات وموفري خدمات الحل. وفي عالم توجيه عناوين IP، فإن شركائنا في تلك المناقشات والأبحاث يميلون لأن يكونوا سجلات الإنترنت الإقليمية (RIR) وفي بعض الأحيان موفري خدمة الإنترنت، إلخ.

إذن فهذه منطقة مختلفة بالنسبة لنظام أسماء النطاقات، لكننا لا نتعامل فقط مع نظام أسماء النطاقات.

واسمحوا لي أن أحيل الكلمة إلى ديفيد من أجل الحديث قليلاً حول بعض من هذه المسائل.

ديفيد هوبرمان: مرحبًا. هذا سؤال رائع، وهو سؤال نتحدث حوله أحيانًا على المستوى الداخلي أيضًا لأننا لم نرغب أبدًا في تخطي اختصاصنا. لكن الحقيقة تتمثل في إن البنية التحية العامة الأساسية وهذه الفكرة الرائعة حول أمن توجيه مسار البيانات، حيث يقوم موفرو خدمة الإنترنت وجميع

المشاركين في توجيه الإنترنت بتمرير البيانات وتمرير الإعلانات حول ماهيتهم—"على رسلك، هذه شبكتي، وهذه هي الخدمات المتاحة لدي؛ فإذا أردت الوصول إلى هنا، فتعال إلي من خلال هذه الإعلانات الخاصة بتوجيه البيانات"—فعلى مدار 30 أو 40 عامًا لم تكن آمنة تمامًا.

حسنًا، والآن فنحن بصدد تأمينها. فنحن بصدد تأمينها وراء بنية تحتية يمكنها أن تمنع الكثير من الحوادث والكثير من الانتهاكات التي تقرأون حولها أحيانًا. وحيث إننا صناعة قائمة بذاتها، بالطبع، فإننا لا نريد القراءة حول ذلك لأننا لا نريد أن يحدث ذلك بسبب رغبتنا في أن تكون البنية التحتية الأساسية تعمل على هذا النحو، فعندما تقوم بالتقاط وأخذ نصيحتك، يمكنك الانتقال إلى أي من المواقع التي تريدها، ويكون الأمر ناجحًا، ولا يتوجب عليك التفكير في هذا الأمر. إذن لدينا هذه الطبقة من الأمن التي نقوم على بنائها فوق كل ذلك، ويتعين علينا التأكد من الانتهاء منها جيدًا وأنها تتم بالشكل الصحيح.

وفي الوقت نفسه، يجب أن نكون على دراية بحقيقة أن مجمل البنية التحتية للأسماء والأرقام، والتي تقع بالطبع ضمن نطاق اختصاصنا، أنا تقع في الخلف من هذه البنية التحتية للأمن، وأنها خلف طبقة الأمن. وإذا لم يتم الانتهاء منها بشكل جيد ولم نتمكن من الوصول إلى خوادم الأسماء ووحدات حل التصديق، إذا لم نتمكن من الوصول إلى مختلف المكونات التي ننظر فيها، فسوف يمثل ذلك مشكلة، اتفقنا؟ ومن ثم فإننا نولي الكثير من الاهتمام بهذه المسألة.

والآن، هناك سؤال على وجه التحديد حول شركة Meta. وقد سألتم عن الكيفية، منذ أكتوبر/تشرين الأول 2021، كانت موقع شركة فيسبوك غير متاح تمامًا لمدة يوم كامل. وكان السبب في ذلك يرجع إلى نظام أسماء النطاقات. وهناك فكرة سائدة في عالم الإنترنت، بأنه في حالة تعطل أي شيء، فالسبب في ذلك يرجع إلى نظام أسماء النطاقات، لأنه ومن الجدير بالملاحظة أن الخطأ الشائع يرجع إلى نظام أسماء النطاقات.

وهنا، فإن شركة Mata أجرت تكوينًا هامًا للغاية حيث كان الوصول المادي إلى الأبنية مثل الوصول إلى مركز البيانات والوصول إلى مقر شركة فيسبوك ... فقد استخدموا شارات تعريفية، مثل أي شركة أخرى، اتفقنا؟ لكن المنظومة الكاملة كانت مرتبطة بنظام أسماء النطاقات DNS. ولكي تتم المصادقة على هويتك، فقد استخدمت نظام أسماء النطاقات من أجل العثور على المستودعات التي كانت بها تلك المعلومات، اتفقنا؟ لكن كان هناك عطل على المستوى الداخلي. كان هناك عطل على المستوى الداخلي ألقى بظلاله وجعل نظام أسماء النطاقات غير متاح ليس

فقط بالنسبة للعالم ولكن لجميع الأنظمة داخل شركة Mata. معنى هذا أنك عندما قمت بإظهار شارتك عند أحد الأبواب، من أجل توثيقها، فقد احتاجت إلى نظام أسماء النطاقات من أجل التعرف عليك. لكنها لم تحصل على إمكانية الوصول إلى نظام أسماء النطاقات. حسنًا، هذه طريقة إبداعية للغاية في شرح الأشياء.

وما أعتقده أنه لم يعلم ذلك فقط شركة Mata ولكن علمنا جميعًا أن نتفكر فيه، وهو عندما تقوم ببناء بنية تحتية، سواء كانت تقنية معلومات لشركات، أو كان شبكة WAN عملاقة يعتمد عليها الكثير والكثير من الناس من أجل الوصول أو من أجل المحتوى، فيجب عليك فعليًا التفكير في التفاعل بين التوجيه والتوثيق والمصادقة ونظام أسماء النطاقات DNS. ولا تتسبب مصادفة في إحداث أعطال يمكن أن تلقي بظلالها على الغير وتجعل منعزلاً بحيث لا يمكن لأحد الانتقال.

إذن فقد كانت هذه حادثة ملفتة للغاية، وأعتقد أن الجميع تعلم الكثير منها.

جون كرين: وإذا ما نظرنا في المكان المحيط بالاجتماع، فربما تجدون أشخاصًا من شركة Meta حاضرين معنا هنا. فقد كانت الشبكة تابعة لهم والمشكلة تخصهم، وربما يمكنكم اللجوء إليهم وسؤالهم عن رأيهم فيها.

سيرانوش فاردانيان: شكرًا. لأغراض الترجمة الفورية، برجاء التحدث بوتيرة معقولة.

لدينا سؤال من مشارك عن بعد من شانيل ماكبيرسون، أحد المشاركين في برنامج NextGen باجتماع ICANN76. لقد اضطرت لإلغاء مشاركتها في اللحظة الأخيرة، لكن سؤالها مقدم من فريق جون كرين. "كيف يتم نشر الامتدادات الأمنية لنظام أسماء النطاقات DNSSEC، وكيف يمكن لمزود خدمة إنترنت لبلد المشاركة في تنفيذ ذلك؟"

جون كرين: حسنًا، في البداية، شانيل، يؤسفني عدم قدرتك على المشاركة معنا. ولكن أتمنى أن نجتمع معك في المستقبل في مكان ما. وأتمنى أن تواصلي تقديم طلبات من أجل المجيء إلى اجتماع ICANN، وسوف نراك في المرة القادمة.

سوف أحيل الكلمة في البداية إلى كيم من أجل الحديث حول هذا الأمر من جذوره، وبعد ذلك سوف أطلب من ديفيد التحدث قليلاً حول الأعمال التي نقوم بها بخصوص المشاركة حول الامتدادات الأمنية لنظام أسماء النطاقات DNSSEC. إذن كيم، لم لا تتحدث قليلاً حول الجذر؟

كيم ديفيز: شكرًا لك، جون. أحد وظائف IANA التي لم نناقشها إلى الآن هي إدارة منطقة جذر نظام أسماء النطاقات. فمنطقة جذر نظام أسماء النطاقات هي الجزء الأهم في نظام أسماء النطاقات إن جاز التعبير. فهي أول مكان تقصده أجهزة الكمبيوتر الداخلة إلى نظام أسماء النطاقات من أجل العثور على عنوان بصدد البحث عنه. وهي تحتوي على سجل موثق بنطاقات المستوى الأعلى الموجودة ومكان الخوادم المسئولة عن نطاقات المستوى الأعلى تلك الموجودة على الإنترنت.

ويشتمل جزء من مسئوليتنا في إدارة منطقة جذر نظام أسماء النطاقات على إدارة مفاتيح التشفير التي تؤمّن منطقة الجذر للامتدادات الأمنية لنظام أسماء النطاقات. وهو جزء مشمول بشكل خاص فيما نقوم به من عمليات. وفي حقيقة الأمر، لدينا الكثير من الموارد المخصصة فقط من أجل تلك الوظيفة الوحيدة داخل هيئة الإنترنت للأرقام المخصصة IANA. والسبب وراء ذلك بسيط. فالامتدادات الأمنية لنظام أسماء النطاقات تعمل بشكل أساسي من خلال الحصول على مفتاح مركزي واحد يعتمد عليه الجميع في بدء وإطلاق عملية البحث تلك في نظام أسماء النطاقات. ومن الضروري جدًا الاحتفاظ بذلك المفتاح بطريقة آمنة للغاية وجديرة بالثقة ويعترف بها المجتمع وأنها تتم بطريقة لا تمثل أي خطر للوصول غير المرخص إلى ذلك المفتاح.

إذن طريقة القيام بهذا الأمر تتمثل في الحفاظ على أمن وسلامة ذلك المفتاح. فهو جزء من مسئولياتنا. حيث نحتفظ به في اثنتين من منشآتنا الأعلى تأمينًا. وكل ثلاثة أشهر، ننتقل للوصول إلى ذلك المفتاح من أجل استخدامه عن طريق فعاليات عامة للغاية ونطلق عليها اسم مراسم مفاتيح التشفير. ونقوم بإحضار المجتمع معنا. ونجري بثًا مباشرًا له. وهي من المحافل العامة للغاية. لكننا نقوم بذلك بطريقة يمكن لخبراء الأمن على وجه الخصوص مراقبتها ومشاهدة ما نقوم به ويمكنهم المجيء إلينا والقول، "نعم، لقد اتبعت ICANN إجراءً جيدًا هناك، وقامت بذلك

بطريقة لا تمثل أي خطر من حيث استخدام المفتاح بطريقة غير مرخص بها". ويكون الجميع راضون.

إذن وكما قلت لكم، فهذا من الأجزاء الأساسية في عملياتنا التشغيلية. ويمكنني أن أعطيكم وصفًا على مدار ساعة حول الطريقة التي يعملون بها. فهذا من الموضوعات الشيقة للغاية. لكنه واحد من المسئوليات الأساسية للغاية التي تقع على كاهل هيئة الإنترنت للأرقام المخصصة وبالتالي على ICANN بالنسبة لأمن الامتدادات الأمنية لنظام أسماء النطاقات.

لكنني أشير إلى أن السؤال كان حول ماهية موفر خدمة الإنترنت في سياق الامتدادات الأمنية لنظام أسماء النطاقات. ومن ثم سوف أحير الميكروفون من أجل الحديث قليلاً حول ذلك الأمر.

ديفيد هوبرمان: بالتأكيد. بعد قيام فريق كيم بعمل رائع في تأمين تحديث الامتدادات الأمنية لنظام أسماء النطاقات وأنها تعمل في منطقة الجذر، عندئذ يجب علينا استخدامها. حسنًا، كيف يمكننا استخدامها؟ حسنًا، ننقل إلى المستوى التالي مباشرة، ألا وهو نطاق المستوى الأعلى: .com و.org و.museum. وهنا، أود أن أسلط الضوء على أكواد الدول. نحن الآن في المكسيك: .mx. لذلك إذا أردنا إعداد الامتدادات الأمنية لنظام أسماء النطاقات في المكسيك لأي نطاق يخضع إلى نطاق المستوى الأعلى .mx، فإننا ننتقل إلى السجل—أي مشغل السجل لنطاق .mx. وذلك أن مشغل السجل يقوم بتوقيع منطقته ويعرض توقيع الامتدادات الأمنية لنظام أسماء النطاقات DNSSEC وتوثيقها لكل نطاق تحت إدارته.

ومن ثم فإنني أتطلع إلى الجمهور، وأرى زميلي، نيكولاس أنطونيلا. نيكولاس مقيم الآن في الأوروغواي في أمريكا الجنوبية ... وما يقوم به نيكولاس هو أنه يدور حول موفري خدمة الإنترنت المختلفين ومشغلي سجلات نطاقات المستوى الأعلى لرموز البلدان المختلفين، وسوف يعمل معهم من أجل إعداد توقيع الامتدادات الأمنية لنظام أسماء النطاقات DNSSEC، من أجل تعليمهم حول كل ما يحتاجون معرفته حول الطريقة التي يعمل بها، وعلى وجه الخصوص، الأدوات التي يحتاجونها من أجل الحفاظ على ذلك. ويمكنه العمل مع موفري خدمة الإنترنت من أجل ضمان قيامهم بتوثيق وحدات حل التصديق الخاصة بهم، بحيث عندما يتم توقيع الامتدادات الأمنية لنظام أسماء النطاقات، فيمكنهم توثيق توقيعاتهم وتمريرها.

ومن ثم تعمل ICANN في مستوى الجذر لضمان أن كل شيء موقع وضمان قدرة الجميع على التوثيق استخدام المفاتيح. وبعد ذلك، تعمل ICANN أيضًا مع موفري خدمة الإنترنت ومع مشغلي السجلات لضمان حصولهم على جميع المعلومات والمعرفة وجميع الأدوات وجميع أشكال الدعم الذي يحتاجونه من أجل عرض الامتدادات الأمنية لنظام أسماء النطاقات في المستويات التالية.

سيرانوش فاردانيان: شكرًا.

سيتونجي، أعتقد أنك رفعت يدك.

شكرًا لك، بيتين على مساعدتي.

وبعد ذلك، أوليفيه، سوف نعود إليك وإلى فيروز.

سيتونجي هونزانجي: أود التحدث باللغة الفرنسية، رجاءً. شكرًا. أنا اسمي سيتونجي. وأنا أحد مسئولي النظام، وأنا أدير خادم لينكس. وأنا من دولة بينين، وأعيش في فرنسا.

وسؤالي حول نطاقات ccTLD. فأنا مهتم بكل شيء يخص نظام أسماء النطاقات، حيث أعمل على كيفية تأمين خوادم نظام أسماء النطاقات. وسؤالي يتعلق بنطاقات المستوى الأعلى لرموز البلدان ccTLD لأنه ولعلكم تعلمون في العديد من الدول، فإن نطاقات ccTLD والسجلات يتم اختيارهم بموجب قرار حكومي. وقد لاحظنا في الكثير الغالب أن نطاقات ccTLD يتم تكوينها بشكل غير جيد، وتدار ويتم الإشراف عليها بشكل غير جيد. ومشكلتي تتمثل في التعرف على ما إن كان من الممكن جعل ICANN تدقق جميع نطاقات ccTLD من أجل إصدار قواعد حول ما يجب القيام به. وأنتم تعلمون أن هناك حاليًا الكثير من نطاقات ccTLD لم تقم بتنفيذ الامتدادات الأمنية لنظام أسماء النطاقات. إذن ما الذي تقوم به ICANN؟

أود من ICANN أن تجبر الناس. إذن على سبيل المثال، يمكنكم إطلاق عملية تدقيق على بعض نطاقات ccTLD، ثم تقولون لهم "أنظمتكم غير حديثة، ولا يمكننا مواصلة إجراء الأعمال معكم. وسوف نرسل لكم مدققًا. وسوف نفرض بعض الأشياء بحيث يمكنكم تحديث أنظمتكم"، لأنه إذا

ما تم تأمين نطاقات ccTLD الأوروبية والأمريكية وليس الإفريقية، فهذه مشكلة. وقد قلنا أن ICANN هي عالم واحد، وإنترنت واحد، لذلك لا يمكن أن نحصل على عالم واحد وشبكات إنترنت متعددة.

كان هذا هو سؤالي. شكرًا.

جون كرين: حسنًا، لقد قسمت ذلك إلى قسمين. الأول وجود بعض البيانات حول حالة بيئة نطاقات ccTLD والحالة الفنية لها. وقد ألقيت بعض التعليقات الملفتة هناك، لكنني أود أن أطلق مناقشة جانبية حول ذلك لأنني أود أن أعرف ما هي البيانات التي لديك، لأننا بصفتنا باحثين وعلماء فإننا مهتمون فعليًا بالبيانات. إذن لقد طرحت العديد من البيانات والمعلومات هناك حول جودة البنية التحتية، وإذا كانت لديك بيانات تدعم ذلك، فنود الحصول عليها. وإن لم يكن الأمر كذلك، فنود إجراء مناقشة حول ما هو مرئي وما هو غير مرئي. وكان أحدها أنك ذكرت أن العديد من نطاقات ccTLD غير موقعة. وأعتقد أن هذا رأي شخصي لأن هناك الكثير منها موقع بالفعل. ومن ثم يمكننا إجراء مناقشة حول البيانات.

الأمر الآخر لم يكن حول مشكلة فنية على الإطلاق في حقيقة الأمر ولكن المشكلة الخاصة بالسياسة حول الكيفية التي تدار بها نطاقات ccTLD. والآن، فإن نطاقات ccTLD ليس لها سياسة موضوعة من جانب ICANN أو داخل ICANN، ولكن نطاقات ccTLD عبارة عن أكواد للدول، ولها آلية مختلفة. ومن ثم فليست هناك آلية متاحة أمام ICANN من أجل المضي قدمًا وفرض سياسات خاصة في هذه الناحية. فهو ليس موجودًا. فما نقوم به هو أننا نتعاون كثيرًا—أعني كثيرًا—مع نطاقات ccTLD. ويمكن لديفيد الحديث حول مقدار العمل الذي نقوم به مع نطاقات ccTLD.

إذن على وجه التحديد فإن منتديات مثل ICANN هي مكان يمكننا الاجتماع فيه ومناقشة هذا النوع من المشكلات ومناقشة مشكلات السياسة. أما منظمة دعم أسماء رموز البلدان ccNSO فهي المكان الذي تجتمع فيه نطاقات ccTLD وتعمل على جميع أنواع هذه المشكلات. كما أن لديهم يوم فني مخصص في غالبية اجتماعات ICANN، إن لم يكن في جميعها، حيث يناقشون هذه المشكلات.

إذن هناك الكثير من أشكال التعاون فيما بين نطاقات ccTLD ومع ICANN وعلى وجه الخصوص بعض من فريقي حول تحسين الأشياء، ولكنني أعتقد أن عملية التدقيق بالنسبة لنا تتطلب ملكية وحيازة عملية السياسة تلك. وهذه العملية الخاصة بالسياسات غير موجودة داخل ICANN.

إذن لا، لن يكون هناك، في المستقبل المتوقع أي موقف يمكن فيه لـ ICANN الدخول إلى سجل لنطاقات ccTLD وإجراء عملية تدقيق. ومن خلال الطريقة التي توضع بها السياسات، يمكن للمرء القول بأنه يجب ألا يكون ذلك موجودًا لأنه ليس من اختصاصنا. وهذا ليس دورنا.

كيم، لا أدري إن كان لديك أي شيء تود إضافته، أو ...

كيم ديفيز: نعم. أعتقد أن هذا كان ملخصًا جيدًا. وأعتقد أن من الجدير إعادة التأكيد (لأن هذا الأمر قد لا يكون معروفًا بالنسبة للعديد من الحاضرين هنا) على الاختلاف بين نطاق المستوى الأعلى العام (نطاق gTLD) ونطاق المستوى الأعلى لرمز البلد. بالنسبة لنطاقات المستوى الأعلى العامة، فإنا غالبية أعمال السياسة التي تتم في اجتماعات ICANN مثل هذا الاجتماع تدور حول وضع قواعد ومتطلبات ما هو مطلوب لإدارة نطاقات المستوى الأعلى العامة gTLD والمعلمات التي تعمل من خلالها. وثمة جانب هام في أعمال ICANN وهو أنه بمجرد تقرير المجتمع للقواعد، تنفيذ تلك القواعد ثم مراقبة الالتزام بتلك القواعد. إذن لدى ICANN إدارة للامتثال التعاقدي. ويجب على كل مشغل لنطاق gTLD استيفاء بعض المتطلبات لكي تكون له القدرة على مواصلة تشغيله بنجاح. وإذا لم يستوف ذلك المؤشر لفترة زمنية مطولة، فثمة تعويضات وتصحيحات متاحة لذلك الأمر.

يبدو الأمر وكأنك تسعى للحصول على نوع من الترتيبات مثل هذه، وربما بالنسبة لنطاقات ccTLD، لكن بالنسبة لنطاقات ccTLD، فهذه علاقة مختلفة للغاية. نعود إلى البداية الأولى لنظام أسماء النطاقات، ونعود إلى فترة 1980، فقد تم إصدار قرار—أي قرار تم الاحتفاظ به إلى الآن—بأن يتم منح نطاقات ccTLD فعليًا داخل الدول المقابلة لها. إن دور ICANN محدود نسبيًا: متمثلاً في التوصل إلى وصي داخل الدولة التي ستدير نطاق ccTLD للصالح العام داخل تلك الدولة. ويتمثل المفهوم في أنه داخل تلك الدولة سوف تكون هناك جميع آليات المراقبة ذات

الصلة لضمان بقاء المشغل مسئولاً وأنه يقوم بما هو ضروري. وبشكل واضح، فإن هذا عالم معقد، حيث يمكن لأي عدد من الدول المختلفة الحصول على آليات مختلفة من أجل هذا الأمر. وبعضها أفضل من الآخر. هذا واضح بالطبع.

وأعتقد أن ما يمكن لـ ICANN القيام به بشكل إيجابي من خلال أنشطة المشاركة الفنية لدينا وأشياء من هذا القبيل هي تعزيز أفضل الممارسات من أجل إجراء عمليات بناء القدرات، والمساعدة في إخطار مديري نطاقات ccTLD بماهية الالتزامات المفروضة عليهم وكيفية إنجاز تلك الالتزامات. وهذا أحد المكونات القوية والأساسية لنطاقات ccTLD في إدارتها داخل الدولة، وأن المشغلين ليس لديهم السيطرة والإدارة الكاملة ولكنهم مسئولين بشكل كبير على المستوى المحلي عن الطريقة التي تدار بها. وهذا يعني أن مهمتنا واختصاصنا محدود نسبيًا عندما يتطرق الأمر إلى نطاقات ccTLD. شكرًا.

سيرانوش فاردانيان: شكرًا.

هل لدينا بعض [الأسئلة] هنا؟

حسنًا. سوف نتناول سؤال واحد آخر من هنا وبعد ذلك سؤال من مشارك عن بعد وبعد ذلك سوف نتيح الفرصة أمام كيم من أجل تقديم عرضه التوضيحي. وسوف نواصل [ألعاب الحلوى].

أوليفيه ريستسكي: مرحبًا، أنا أوليفيه. أنا من مقدونيا. وأنا أعمل لدى وزارة الداخلية. وأيضًا، فأنا أحد المشاركين في مركز أبحاث الأمن. وسؤالي يتعلق بمسألة أننا مؤخرًا تعرضنا إلى تلقى رسائل بالبريد الإلكتروني تحتوي على قنابل وهمية في المدارس العامة والمطارات ومراكز التسوق ومراكز النقل والمواصلات. وهي تكلف الكثير من إنفاق الموارد بالنسبة للوزارة التي أعمل فيها. كما أن تعقب هذه الجريمة بطيء للغاية. وبشكل فعال فإن تقصي/تحري هذه الجريمة بطيء للغاية. إضافة إلى ذلك، فإن هذه القضية شائعة للغاية بالنسبة لجميع [يتعذر تمييز الصوت] البلقان. هل هناك أية إمكانية لإجراء أبحاث فيما يخص هذه المشكلات؟

جون كرين: يبدو أنك تتحدث في الأغلب عن عمليات استغلال التصيُّد، إلخ، والبرامج الضارة وأشياء من هذا القبيل وهي أشياء مقيتة وهي جزء من حياتنا اليومية على الإنترنت. نعم، يمكننا إجراء الأبحاث حول ذلك عندما يتعلق الأمر بنظام أسماء النطاقات.

وأنا لا أدري، سامانا، إن أردت الحديث حول ذلك قليلاً عن بعد الأبحاث التي نقوم بها.

سامانا تاج علي: شكرًا لك على سؤالك، أوليفييه، وشكرًا لك، جون. إذن كما قال جون، فهذه مشكلة نموذجية يعايشها يوميًا غالبية مستخدمي الإنترنت. ونحن في الوقت الحالي في مجموعة الأمن والاستقرار والمرونة نجري أبحاثًا حول ذلك. وسوف يتم نشرها قريبًا: تحديد الطرق أو الطرق الأكثر فاعلية في تصنيف رسائل التصيُّد البريدية إلى فئات مختلفة من البريد غير المرغوب والبرامج الضارة إلخ، لذا أرجو مواصلة النظر في وثائق أو منشورات مكتب المسئول الفني الأول. فنحن نخطط لنشر الطرق التي نتبعها. في البداية، سوف نخوض أعمال النشر الأكاديمي، ولكن بمجرد الانتهاء من مراجعة النظراء لها، سوف نقوم بنشر الطرق. وربما يكون من المفيد تنفيذ الطرق في مناطق أخرى أو موفرين ومشغلين، إلخ.

جون كرين: وهناك أشياء أخرى يمكنكم التفكير فيها. والآن، إذا كان لديكم فريق الاستجابة لطوارئ الكمبيوتر على المستوى الوطني، فتأكدوا من أنهم عضو في منتدى الاستجابة للحوادث وفرق الأمن، وهي هيئة تضم فرق الاستجابة لطوارئ الكمبيوتر من جميع أنحاء العالم. وICANN في حقيقة الأمر عضو في منتدى الاستجابة للحوادث وفرق الأمن، وهي منتدى يضم المتفاعلين الفوريين للحوادث. لذلك أرجو منكم المشاركة في ذلك المجتمع. وتأكدوا أن المتفاعلين مع الحوادث موجودون في مجتمع الاستجابة للحوادث لأن هذه المشكلة ليست فريدة لأي أحد.

أما الأمر الآخر الذي يمكنكم القيام به على المدى الطويل هو الاستثمار في جامعاتكم في بناء المهارات وفي الدولة من أجل فهم كل ذلك، سواء كان ذلك بحثًا أو استجابة لحادثة أو حتى مهارات جيدة في تدعيم شبكة العلاقات، إلخ، كما في تدعيم شبكة العلاقات الفنية. وهذا أمر آخر يمكنكم القيام به.

والآن، إذا كنتم مهتمين فعليًا وبشكل أساسي بجوانب السلامة العامة لما تستخدم فيه الإنترنت وتتساءلون عن طريقة الإنفاذ أو كنتم مشاركين في أعمال السياسة في ذلك العالم، فإن لدينا لجنة استشارية حكومية. وهي جزء هام للغاية في عمليات وإجراءات ICANN. وفي كل ذلك، فإن لديهم بالفعل مجموعة عمل يطلق عليها اسم مجموعة عمل السلامة العامة. لذلك إذا كانت حكومتكم مشاركة في اللجنة الاستشارية الحكومية GAC، وكان لديهم اهتمام نوعي بهذه الناحية، فإن مجموعة عمل السلامة العامة هي المكان الذي يمكنهم فيه والمشاركة فيه.

والآن، فإننا في ICANN نركز على شيء نطاق عليه اسم الانتهاك الفني أو التهديدات الأمنية المرتبطة بنظام المعرّفات. ومن ثم ليست جميع التهديدات التي ترونها على الإنترنت—في حقيقة الأمر، العديد من التهديدات التي ترونها على الإنترنت—غير مرتبطة بالعمل الذي تقومون به. لكن هذا الموضوع الخاص دائمًا ما يكون موضوعات ساخنًا في ICANN. وفي هذه اللحظة، هناك أشياء متعددة تحدث داخل المجتمع. فهناك مفاوضات تعاقدية تحدث حول ما يقصد به السجل وأمين السجل وما يعتين عليكم القيام به حيال انتهاك نظام أسماء النطاقات DNS. حيث ينص العقد الحالي على ضرورة حصولك على التقارير والتحري عنها. وهذه ليست نفس الكلمات الواردة في العقد، لكنني لست محاميًا. لكن من بين الأشياء المفقودة من صياغتنا التعاقدية هو أن هؤلاء الأشخاص يجب عليهم الحد من الانتهاكات. ونحن نعمل بوصية من الأطراف المتعاقدة— أي السجلات وأمناء السجلات. إذ لجأوا إلينا وقالوا، "نريد إضافة هذا إلى عقدنا، ومن ثم فإننا ملتزمون تعاقديًا بالحد من الانتهاكات". فالمناقشة جارية في الوقت الراهن.

ونجري الكثير من التدريبات. حيث تقوم سامانا ومجموعتنا بالكثير من الأبحاث والمنشورات في هذه الناحية. إذن فهذا من الأشياء التي نهتم بها كثيرًا جدًا.

وإذا كان لديكم جهات لإنفاذ القانون تود التحدث إلينا حول التعليم والتوعية، فيسرنا التحدث إليهم. ومعنا بعض الأشخاص في فريق عملنا يقضون الكثير من الوقت في التحدث إلى جهات إنفاذ القانون في جميع أنحاء العالم. إذن اختصاصنا الأساسي يتمثل في أن نوضح لهم الطريقة التي تعمل بها المنظومة، وفي بعض الأحيان يتعلق الأمر بإجراء الأعمال التعريفية فيما بينهم والآخرين في المنظومة، وبناء الثقة، إن شئتم، لأن هذا من الأشياء الحيوية بالنسبة لقدرتنا على القيام بالأعمال لصالح الجميع.

إذن لا تترددوا في المجيء إلينا والتحدث معنا، ويمكننا إجراء مناقشة بين فرد وآخر ربما حول طريقة تقديمنا المساعدة إلى وزارتكم وحكومتكم من أجل الانخراط والمشاركة أكثر.

سيرانوش فاردانيان: شكرًا.

هل يمكنني مطالبة الفريق الفني بإظهار العرض التوضيحي الخاص بهيئة الإنترنت للأرقام المخصصة؟

وفي الوقت ذاته، سوف أطرح الأسئلة من المشاركين عن بعد. روملو تشاسين، أحد المشاركين في برنامج NextGen يود أن يعرف الطريقة التي تتفاعل بها مختلف مشروعات وبرامج الحد من التهديدات الأمنية فيما بينها"—وفيما بين بعضها الآخر، أعتقد ذلك.

جون كرين: ما مقدار ما لدينا من وقت؟ أعني أنه إذا ما نظرتم إلى اختصاص ICANN الأساسي، وإذا ما نظرنا في لوائحنا، وإذا ما نظرنا في غرض ICANN، فإنها تؤكد بوضوح شديد أنه ينبغي علينا القلق حيال أمن واستقرار ومرونة الإنترنت أو لأنظمة المعرّفات. إذن ليست هذه هي مواقع ويب الناس، إلخ، لكنه الاسم الذي. مرحبًا. مرحبًا بالجيران. أنا أسمع ... ماذا، أسمع أصواتًا.

إذن بطريقة أو بأخرى، فهي تمثل أساس وجوهر كل ما نقوم به. ومن ثم فإن كل شيء يتفاعل مع الأمن. وفي كل مرة في ICANN باعتبارنا فريق العمل وأيضًا في غالبية الأوقات بصفتنا مجتمع عندما ننظر في شيء ما، دائمًا ما يكون لدينا ذلك الأمر في أذهاننا. كيف يؤثر ذلك على الأمن؟ كيف يؤثر ذلك على الاستقرار؟ إذن كل شيء يتفاعل.

والآن، وداخل مجموعتنا—وقد قمت بتعريفكم بمجموعة من الأشخاص داخل مجموعة المعرفات والبحث والعمليات والأمن—تجري هيئة الإنترنت للأرقام المخصصة IANA عملها بشكل جيد، وهو ما يقومون به دائمًا لأنهم متميزون، وهذا أمر ضروري بالنسبة لأمن النظام ولاستقرار النظام. ويجب أن يكون لدينا تسجيل جيد للمعرفات. وبعد ذلك نقوم بإجراء بعض الأبحاث ونقوم بأعمال التوعية والتعليم. إذن هذا هو العمل الذي نقوم به. لكن معنا أيضًا -كما قال كيم- إدارة الامتثال بالعقود الخاصة بنا. ولدينا مفاوضات خاصة بالعقود. ولدينا تمكين جميع هذه المناقشات

الخاصة بالسياسات. ولكل شيء تأثيره على أمن واستقرار أنظمة المعرّفات لأنه عندما يتطرق الأمر إلى ذلك فهذه هي مهمتنا ووظيفتنا. هذا هو عملنا الذي نقوم به.

سيرانوش فاردانيان: شكرًا.

كيم، هل يمكنني أعضاء الكلمة إليك من أجل التعريف بأعمال هيئة الإنترنت للأرقام المخصصة، رجاءً.

كيم ديفيز: بالتأكيد. إذن يبدو الأمر وكأنه فرصة جيدة، في حين أنن نجري هذه المناقشة، فقط من أجل إجراء جولة سريعة للتعرف على ماهية وظائف IANA. وهذا من الأشياء التي ربما تكونوا قد سمعتم بها كثيرًا خلال أحد اجتماعات ICANN. كما أن مصطلح "IANA" منتشر للغاية، على افتراض أنكم تعرفون المقصود منها. إذن من المقرر أن يكون هذا نظرة عامة موجزة نسبيًا على ما تتألف منه وظائف IANA. وأتمنى أن يضيء ذلك لكم الطريق، أيضًا. وسوف نستأنف الأسئلة بعد ذلك. فإذا ورد إلينا أي شيء وتودون منا تناوله بالتفصيل، فلا تترددوا في إبلاغنا به.

تحدثنا قليلاً حول هذه المسألة بالفعل: IANA هيئة الإنترنت للأرقام المخصصة. على الرغم من الاسم، فإننا نتعامل مع أكثر من الأرقام. حيث نتعامل مع الأسماء أيضًا. ونتعامل مع معلمات البروتوكولات. ونتعامل مع جميع أشكال المعرّفات المختلفة.

ومن حيث الجوهر، فهذا أحد أقدم المعاهد الموجودة حول العالم. فبالعودة إلى الأيام الأولى على نشأة الإنترنت، عندما كان مجرد مشروع بحثي، عندما تم توصيل تلك العقد الأولى في أواخر ستينيات وأوائل سبعينيات القرن الماضي، توجب على شخص ما الاحتفاظ بسجلات حول هويات أجهزة الكمبيوتر وهويات أصحابها. وقد تم تأدية ذلك الدور في فترة مبكرة للغاية من خلال شخص اسمه جون بوستل. وهو الشخص الموجود إلى اليمين في الفيديو بجوار فينت سيرف. وقد كان جون بوستل هو التجسيد الشخصي لهيئة IANA في البداية الأولى.

ولاحقًا، حصلت هيئة الإنترنت للأرقام المخصصة على اسمها وباتت جزءًا من اسم تم إطلاقه في فترة ثمانينيات القرن الماضي. وقد حققت IANA نموًا لكي تكون أكثر من مجرد شخص واحد. فتحولت إلى فريق.

ولكن في نهاية المطاف، كان ذلك هو الغرض الأصلي في ذلك الوقت وما يزال هو الغرض القائم حاليًا: ما المعرّفات المستخدمة، وهل هناك سجل رسمي يحدد المعرّفات التي تم استخدامها في ذلك؟

ومن ثم في فترة تسعينيات القرن الماضي، تم الإقرار بأن وظائف IANA على وجه الخصوص وإدارة منطقة الجذر بحاجة فعلية إلى شكل من أشكال الهياكل الرسمية أكثر من مجرد شخص أكاديمي (جون بوستل كان يعمل في جامعة) وأبعد مما كان بإمكانه القيام به على المستوى الفردي ومع الفريق الخاص به. وقد كانت هناك جهود طوال فترة التسعينيات من أجل نشر ذلك، ولإدراك وتحقيق إضفاء السمة التجارية على الإنترنت، ونمو الإنترنت، وزيادة الطلبات على وظائف IANA.

وقد تم إنشاء ICANN لتكون هي مقر لهيئة الإنترنت للأرقام المخصصة IANA. وقد كان هذا هو اختصاصها الأصلي. وفي حقيقة الأمر، قبل أن تحصل ICANN على اسمها، فقد كان يطلق عليها اسم IANA الجديدة. وما تزال ICANN موجودة حتى يومنا هذا من أجل ذلك الغرض الأساسي. ولدى ICANN اختصاصات أخرى للمعرّفات تتجاوز مجرد أعمال IANA، لكن ما تزال أعمال هيئة الإنترنت للأرقام المخصصة هي المهمة الجوهرية لـ ICANN.

إذن ICANN اليوم عبارة عن إدارة تابعة لـ ICANN، وهي تحتفظ بالسجلات (وأنا أستخدم "السجلات" هنا بالمعنى العام—ليس سجلات النطاقات ولكن السجلات كما ترد في أي سجل رسمي) للمعرّفات الفريدة الخاصة بالإنترنت. ولكل واحد من هذه السجلات سياسة مختلفة، ومن ثم فإن جانبًا من أعمال فريقنا يتمثل في تطبيق تلك السياسات استنادًا إلى نوع المعرّف والموقف الواردة فيه. ومن ثم عندما تسمعون كلمة ""IANA، فهي تشير إلى هذه الوظيفة الخاصة بالتخصيص، وهذه الوظيفة الخاصة بالحفاظ على السجلات والتي تقوم على تشغيلها إدارة IANA داخل ICANN.

إذن ما سبب الحاجة إلى أمين سجلات رسمي مثل IANA من أجل الإنترنت؟ أليست الإنترنت خالية من أي رقابة وتحكم مركزي؟ إن أجهزة الكمبيوتر تتحدث إلى بعضها الآخر من خلال استخدام بروتوكولات فنية، ومن الضروري فعليًا أن تكون تلك البروتوكولات الفنية متطابقة بحيث تفهم أجهزة الكمبيوتر بعضها الآخر. وفي حين يتم نقل المحتوى عبر تلك البروتوكولات، فإن تلك البروتوكولات الأساسية هي أشياء مثل TCP/IP، على سبيل المثال.

ويتعين عليهم العمل بنفس الطريقة على كل جهاز لكي تعمل الشبكة وحسب، ومن ثم فإن الكثير من العمل الذي نقوم به في IANA لا يتعلق كثيرًا بالبروتوكولات التي ترونها، مثل أسماء النطاقات، ولكن الأشياء التي تعمل أسفل ذلك في المستوى الأدنى من جهاز الكمبيوتر وفي أجهزة توصيل الشبكات لضمان أن النقل فيما بين أجهزة الإنترنت المختلفة يعمل ودقيق، وأن مرفقات الملفات التي يتم إرسالها تصل ويتم استلامها في الجهة الأخرى بالنسق الصحيح، وأنه عندما تقوم بالاتصال بجهاز، لا تحصل على مكالمة صوتية بدلاً من موقع ويب. وأشياء من هذا القبيل. إذن كل هذه المعرِّفات لها غرض خاص يتمثل في مساعدة ذلك الاتصال. وهي تستخدم بشكل أساسي من خلال موفري البرمجيات. ويستخدم موفرو البرمجيات تلك التعيينات من جانب IANA لضمان أن البرمجيات الخاصة بهم تعمل مع الغير على الإنترنت.

ومن ثم فإن الوظائف تدار اليوم من خلال فريق IANA. وهناك العديد من العقود المختلفة. وهي تمثل فوضى معقدة من العقود، كي أكون أمينًا معكم، لكن على الرغم من ذلك، هناك الكثير من العقود التي تحكم الطريقة التي تؤدي بها وظائف IANA اليوم.

وثمة مصطلح آخر قد تعرفونه أو ربما سمعتم به هذا الأسبوع وهو PTI أو هيئة المُعرِّفات الفنية العامة. علمًا بأن هيئة المُعرِّفات الفنية العامة جهة تابعة لمنظمة ICANN. اعتبروا أنها جهة فرعية تابعة لـ ICANN تقوم في حقيقة الأمر بأداء وظائف IANA. وبالنسبة لغالبية المقاصد والأغراض، فإن هيئة المُعرِّفات الفنية العامة لا تمثل اختلافًا كبيرًا. فمن بين الضمانات التي تم تنفيذها في عام 2016 عندما تم إجراء نقل أصحاب المصلحة المتعددين لـ ICANN تمثل في وضع وظائف IANA في مؤسسة مختلفة عن ICANN لكن يجب أن تكون مؤسسة تخضع لإدارة ICANN، وكان ذلك هو هيئة المُعرِّفات الفنية العامة. إذن سوف تسمعون عن هيئة المُعرِّفات الفنية العامة PTI. نصيحتي هي: لا تقلقوا كثيرًا بشأن مصطلح PTI أو هيئة المُعرِّفات الفنية العامة. فقط اعلموا أنها الاسم القانوني الرسمي للكيان الذي يدير وظائف IANA.

العمليات اليومية؟ ونحن نعمل تمامًا مثل أي إدارة في ICANN. إذن نحن حوالي 16 شخصًا، وهذا هو أساس عملنا. هذا هو ما نقوم به في وظيفتنا.

إذن ما هي وظائف IANA بمزيد من التفاصيل أكثر؟ بشكل نموذجي، فإننا نقسمهم إلى ثلاثة أقسام: معلمات البروتوكولات وموارد الأرقام وأسماء النطاقات. وهذا التقسم اعتباطي إلى حد ما. فثمة تداخل فيما بين هذه القطاعات. لكن بالنسبة لمناقشة رفيعة المستوى حول وظائف IANA، من المفيد بشكل جيد تقسيمها إلى ثلاث نواحي.

الناحية الأولى التي سوف أركز عليه هي معلمات البروتوكولات لأنها بشكل أساسي الجانب الأهم على الإطلاق فيما نقوم به. معلمات البروتوكولات. وهناك آلاف الأنواع المختلفة من معلمات البروتوكولات. وهناك مئات الآلاف إن لم يكن الملايين من تعيينات معلمات البروتوكولات. فأعدادها لا تحصى. وهناك الكثير منها. حتى أن نسبة 99% منها لم يسمع بها أي أحد منكم من قبل. ونسبة 98% منها لم أسمع أنا بها من قبل. فهناك الكثير. والكثير منها يستخدم في تطبيقات نوعية للغاية. وما لم تكن بصدد إنشاء برمجيات للقيام بعمل نوعي ومخصص للغاية، فقد لا تحتاج على الإطلاق إلى استخدام واحد من هذه السجلات. لكن بالنسبة لخمسة أو عشرة أو 50 شخصًا يعملون في صناعة مخصصة للغاية وتقوم بتنفيذ برمجيات حول واحدة من مجموعات المعرّفات الفريدة تلك، فإن العمل الذي تقوم به هيئة الإنترنت للأرقام المخصصة لا يقدر بثمن. وثمة مسرد في IANA.org/protocols إن أردتم الاطلاع على القائمة الكاملة، لكن هناك الكثير منها هناك.

بالنسبة لمعلمات البروتوكولات، تؤدي هيئة IANA دورًا مباشرًا في وحدات التنفيذ تلك، والتي غالبًا ما تكون عبارة عن موفري برمجيات ومطوري بروتوكولات، يأتون مباشرة إلى IANA، ويتحدثون إلى فريق العمل، ويحصلون على المخصصات التي يحتاجونها منا مباشرة. وهذا هو العنصر المميز الأساسي عن أسماء النطاقات وموارد الأرقام التي سوف أتطرق إليها بعد قليل، لأن الناس بشكل عام لا يأتون إلى هيئة الإنترنت للأرقام المخصصة من أجل الحصول على اسم نطاق. كما أن الناس لا يأتون إلى IANA من أجل الحصول على مورد أرقام. وعوضًا عن ذلك، فإن لديهم هذه الأنظمة الخاصة بالتخصيص الهرمي حيث يكون هناك وسيط. وهناك أشخاص مختلفون ولديهم مسئوليات مختلفة. وتؤدي IANA فقط جزء بسيط من عملية التخصيص هناك.

وجزء من السبب وراء ذلك يتمثل في أن هناك الكثير من السياسات التي تنطبق على موارد الأرقام وعلى أسماء النطاقات.

إذن من أين تأتي سجلات معلمات البروتوكولات هذه؟ فالغالبية العظمى منها يتم تطويرها في IETF (فريق عمل هندسة الإنترنت). وهي الهيئة الأساسية المعنية بوضع المعايير للإنترنت. وهي تتعلق أكثر بالمكان الذي تجري فيه أعمال وضع معايير الإنترنت—ليس جميعها ولكن الغالبية منها. وعندما يقوم النسب بوضع المعايير الخاصة بالإنترنت في فريق عمل هندسة الإنترنت، يقوم جزء من ذلك بتطوير سجلات IANA لكي تتماشى مع معايير الإنترنت تلك.

وربما تكونوا قد سمعتم بلفظ RFC أو طلبات الحصول على تعقيبات. وهي عبارة عن سلسلة وثائق يتم فيها نشر معايير الإنترنت. والعديد من طلبات RFC إما تقوم بإنشاء أو الإشارة إلى أو تعديل سجلات IANA. وهي تشتمل على تعليمات حول ما ينبغي على IANA القيام به والسياسات التي يتوجب عليها إنفاذها.

وللحديث قليلاً حول موارد الأرقام، بالنسبة لمن لا يعرفونها، فإن موارد الأرقام تشير في المعتاد إلى ثلاثة أشياء رئيسية: عناوين بروتوكول الإنترنت الإصدار 4، وعناوين بروتوكول الإنترنت الإصدار 6 وأرقام النظام المستقل. بالنسبة لمن هم غير ملمين بعناوين بروتوكولات الإنترنت، فهناك إصداران: الإصدار 4 والإصدار 6. لكن هذه أرقام فريدة والتي يتم تخصيصها لكل جهاز على الإنترنت. وجهاز الكمبيوتر المحمول الخاص بك له واحد. وهاتفك به واحد. وجهازك الذكي في المنزل يحتوي على إحداها. وربما جهاز التلفاز يحتوي على واحد. وبشكل متزايد، فإن العديد من الأشياء في هذا العالم تحتوي عليها، ألا وهي المعرّفات الفريدة التي تستخدم من أجل النقل من جهاز إلى آخر. وفي صميم هذا الأمر، عندما تتم عملية نقل عبر الإنترنت، فإن كل عملية نقل يطلق عليه اسم حزمة ويجب أن يكون لها عنوان "من" وعنوان "إلى". وعنوان "من" وعنوان "إلى" عبارة عن عناوين IP.

لأنه يوجد حرفيًا ملايين من هذه العناوين، وأنت بحاجة إلى طريقة لتجميعها في مجموعات كبيرة من أجل جعل التعامل معها سهلاً بحيث لا يتوجب على مهندسي الشبكات الكتابة في كل عنوان IP فردي على حدة. وبهذه الطريقة يقومون بذلك مع عناوين النظام الذاتي، أو أرقام النظام المستقل. والطريقة التي أحب أن أنظر بها إلى ذلك حول أرقام النظام المستقل هي أنها تشبه الأكواد البريدية للإنترنت. وسوف يقوم موفرو الشبكات بتجميع مجموعات كبيرة من عناوين IP

معًا في رقم فردي—أي رقم نظام مستقل—وبعد ذلك، عندما يتحدثون حول مكان نقل البيانات عبر الإنترنت، فإنهم يستخدم أرقام النظام المستقل بدلاً من ذلك لجعلها مهمة أكثر سهولة.

إذن فقد تحدثت حول هذه الأشياء. وسوف أشير إلى أن عناوين IP من الإصدار 4-فقد نفدت جميعها. فقد نفدت منا آخر عناوين IPv4 المتاحة منذ بضع سنوات. سجلات الإنترنت الإقليمية التي تخصصها للشبكات قد انتهت ونفد أغلبها. إذن هناك مخزون قليل للغاية من الاصدار الرابع من بروتوكول الإنترنت IPv4، وهذا هو السبب في أنكم سوف تسمعون أن هناك الكثير من المبادرات من أجل الانتقال إلى الإصدار السادس من بروتوكول الإنترنت IPv6، والذي يحظى بقدر أكبر من السعة والقدرة على نمو الإنترنت.

إذن فقد ذكرت للتو سجلات الإنترنت الإقليمية. وبالنسبة لمن هم غير ملمين بالمفهوم، فقد ذكرت من قبل أنكم لا تأتون مباشرة إلى IANA من أجل الحصول على عنوان IP. ما يحدث هو أنك عندما تكون مستخدمًا نهائيًا يتم تخصيص عنوان IP تلقائيًا لك من خلال موفر الشبكة. فهم يستخدمون بروتوكولاً، DHCP—وهو بروتوكول آخر من البرتوكولات التي تعمل عليها IANA خلف الكواليس. حيث يخصص لك DHCP عنوان IP فرديًا لكل جهاز على حدة. وكل موفر شبكة، سواء كان موفر خدمة إنترنت الذي تتعامل معه أو أي شبكة مؤتمر في فندق لديها مجموعة من عناوين IP يشاركونها فيما بين الناس في منشأتهم أو على الشبكة الخاصة بهم.

من أين يحصلون على المجموعات الخاصة بهم؟ حسنًا فهم يلجأون إلى سجل إنترنت إقليمي. حيث إن هناك خمسة من سجلات الإنترنت الإقليمية. وسجل عناوين الإنترنت لأمريكا اللاتينية والكاريبي LACNIC هو سجل الإنترنت الإقليمي للمكسيك هنا. ولكل واحد منها، فإن الشغل الشاغل لها هو تعيين أرقام النظام المستقبل وعناوين IP هذه لمشغلي الشبكة داخل منطقتهم. وتحصل سجلات الإنترنت الإقليمية بدورها على تخصيصاتها من هيئة الإنترنت للأرقام المخصصة IANA.

وأخيرًا أسماء النطاقات. ما دور أسماء النطاقات؟ سوف أتخطي هذا الموضوع. ومن ثم، من حيث الترتيب الهرمي لنظام أسماء النطاقات، فإن الجزء الأكثر حيوية في مساحة أسماء النطاقات هو منطقة الجذر. وهذا جزء أساسي فيما نقوم به في IANA. حيث يمكنكم رؤية أسفل الجذر في هذا الرسم البيانات نطاقات المستوى الأعلى. وبدورها، فإنها تقوم بتخصيص المسميات قبل ذلك، ونطاقات المستوى الثاني، وما إلى ذلك.

ومن ثم فإن مسئوليتنا الأساسية داخل IANA هي إدارة منطقة جذر نظام أسماء النطاقات—وأكرر مرة أخرى، هذا هو السجل الرسمي لما عليه نطاق المستوى الأعلى—وبعد ذلك جميع المعلومات الفنية التي تتوافق مع ذلك وأيضًا المعلومات الإدارية، مثل من هم نقاط الاتصال؟ ما هي الشركة الفعلية التي تقوم على إدارة نطاق المستوى الأعلى ذلك؟ وأشياء من هذا القبيل. إذن نحن القائمون على حفظ السجلات الرسمية لهذه الحقائق. حيث نتلقى طلبات من هؤلاء المشغلين من أجل إجراء تحديثات وتغييرات إدارية على نطاقات TLD الخاصة بهم. ونجري أعمال العناية الواجبة على بعض أنواع الطلبات. وبعد ذلك بمجرد أن ترضى هيئة الإنترنت للأرقام المخصصة IANA بأن أية تغييرات على جذر نظام أسماء النطاقات مناسبة، فإننا نرسلها من أجل التنفيذ في خوادم جذر نظام أسماء النطاقات.

وقد ذكرت لكم هذا الأمر سابقًا نتيجة لطرح الأسئلة، إذن سوف أسرع في هذا الأمر، لكننا نقوم فعليًا بإدارة مفتاح توقيع شفرة الدخول الأساسية، وهو المفتاح المركزي الذي يؤمن نظام أسماء النطاقات أيضًا. ونقوم بذلك مع مراسم توقيع المفتاح الرئيسي. وسبب القيام بذلك بطريقة عامة للغاية هو تعزيز الثقة. ويمكننا القيام بكل أعمالنا من أجل الامتدادات الأمنية لنظام أسماء النطاقات وتأمين الإنترنت بطريقة خاصة والقول "مرحبًا، نحن DNSSEC. ثق بنا"، لكن أفضل طريقة للقيام بذلك هو إشراككم جميعًا في العملية، وإعطاء المجتمع القدرة على الوصول والرؤية. ونحن نعتقد أنه يؤدي إلى تعزيز الثقة بشكل أفضل لأن الجميع بإمكانه أنه يرى بأم عينه. حيث يمكنهم النظر فيما يقومون به، ويمكن لخبراء الأمن من جميع أنحاء العالم النظر فيما نقوم وإلقاء نظرة جماعية على ذلك والقول، "نعم، يجري القيام بذلك بطريقة آمنة ومأمونة. يمكننا الثقة في عمل هذا النظام".

بعض الوظائف الأخرى فقط التي نقوم بها في أسماء النطاقات أيضًا. نحن ندير نطاق .int، وهو واحد من نطاقات المستوى الأعلى. وهذا على وجه التحديد من أجل المنظمات الدولية الحكومية. وهذا ليس متاحًا للتسجيل العام. كما أننا ندير نطاق arpa. لوكالة مشاريع الأبحاث المتقدمة. وسوف ألخص نطاق arpa. بأنه أعمال الأنابيب الفنية. فهذا من النطاقات التي ربما لن ترونها مباشرة، لكنها هامة بالنسبة لبعض عمليات الإنترنت. كما أننا ندير مستودعًا من مجموعات قواعد إنشاء المسميات. هذا هو المكان الذي تشغل فيه السجلات أسماء النطاقات المدوَّلة وتشارك وتلتزم بأفضل الممارسات.

وهذا ملخص وافٍ لعمليات IANA. ومن الواضح أن هذا من الأوصاف رفيعة المستوى للغاية. ولكنني أردت فقط الانتهاء من الأمر بالإشارة إلى الأمن. وفي حقيقة الأمر، أتعلمون؟ وسوف أتجاوز هذه الشريحة. بعض الجوانب الأخرى لهيئة IANA.

وأعتقد أن أهم الأشياء التي نقوم بها هو الحيادية والتجرد. ونحن هنا من أجل تنفيذ السياسات بحذافيرها. ويمكننا توفير النصائح ولكن بطريقة حيادية. فهذا إذن جزء مما نقوم به في مشاركتنا هنا خلال هذا الأسبوع. ولدينا تركيز قوي على الأداء. وهناك الكثير من اتفاقيات مستوى الخدمة التي تحكم ما نقوم به. حيث نقوم باستمرار بقياس ما نقوم به. ودائمًا نقوم بتقديم تقارير حول عملنا ومن ثم لا بأس. ونود إضفاء التحسينات دائمًا، فهذا إذن جزء آخر في عملنا: التحسين المستمر. وجانب من ذلك يتمثل في عمليات التدقيق الخارجية من جهات أخرى وبشكل عام الحصول على مساءلة المجتمع. وهناك الكثير من لجان الإشراف وما إلى ذلك في IANA والتي سوف تتعرفون عليها في مساحة ICANN.

إذن بإيجاز، تحافظ IANA على سجلات أنظمة الترقيم الفريدة. والمهمة المنوطة بهم هي الإبقاء على عمل الإنترنت. وغالبية سجلات هيئة الإنترنت للأرقام المخصصة مباشرة إلى حد كبير. حيث يأتي الناس مباشرة إلى هيئة الإنترنت للأرقام المخصصة IANA. وربما لم تسمعوا من قبل عنهم. فهي سهلة إلى حد ما، إلا أنه يوجد البعض منها رفيع المستوى والمعقد. وقد تحدثنا حول منطقة الجذر. وقد تحدثنا حول المفتاح الذي يحمي منطقة الجذر. وبالنسبة لها، فإن IANA تمثل الجذر العالمي بالنسبة لأنظمة التسمية تلك.

إذن فهذه هي النظرة العامة من ارتفاع 10,000 قدم على هيئة الإنترنت للأرقام المخصصة IANA. شكرًا.

سيرانوش فاردانيان: شكرًا لك، كيم. لقد كانت هذه الكلمة مليئة بالمعلومات المفيدة. وبالنسبة لمشاركينا، فإن هذا العرض عن طريق برنامج باوربوينت تم تحميله على موقع اجتماع ICANN76 تحت تفاصيل هذه الجلسة الخاصة. إذن إذا أردتم تنزيل ذلك الملف واستخدامه، فلا تترددوا في ذلك.

ويمكننا طرح العديد من الأسئلة الآن. فلدينا 30 دقيقة مخصصة لذلك. لذلك رجاءً عدم التردد.

فيروز، أعرف أنك مدرج في قائمة طلبات التعليق. تفضل رجاءً، فيروز. أرى ديفيد؟ نعم. لكننا سوف نبدأ ...

فيروز عظيموف: مرحبًا. أنا اسمي فيروز. وأنا زميل في ICANN. لقد كنت أنتظر ولدي سؤالان بالفعل. سؤالي الأول حول ... وفقًا لما ذكرناه سابقًا حول مشكلة شركة Meta، وأتذكر أنه كانت هنا مشكلة مع شركة Meta حول شبكة Meta الفرعية والإعلان عنها من خلال مزود خدمة إنترنت آخر. وعادة ما يحدث ذلك. فداخل بلادنا كانت لدينا هذه المشكلة: شبكتنا الفرعية المخصصة لنظام DNS تم الإعلان عنها من خلال مزود خدمة إنترنت آخر. وقد فقدنا الإنترنت ليس فقط لهذه المجموعة الفرعية ولكن لجميع المستخدمين لدينا. وسؤالي هو، هل [يتعذر تمييز الصوت] حل يتمثل في منع هذا النوع من المشكلات. وكل جهاز توجيه حدودي على الإنترنت يجب أن يكون به خاصة فحص RPKI ممكنة قبل تثبيت [مسار] في جدول التوجيه. وكيف يمكننا منع ذلك وجعل الاستقرار -كما ذكرتم- في الطبقات السفلى (على سبيل المثال، في الطبقة 3)؟

جون كرين: حسنًا، إذن هذه مناقشة أخرى حول كيفية تأمين التوجيه. وما تشيرون إليه هو ما يشار إليه في الغالب باسم برنامج السطو على بروتوكول البوابة الحدودية BGP.

وسوف أحيل الكلمة إلى ديفيد من أجل الحديث حول هذه المسألة قليلاً.

ديفيد هوبرمان: إذن فن البنية التحية العامة الأساسية RPKI تساعد في هذه المسألة إلى حد ما. والمهم في ذلك هو أن المسألة التي وصفتموها للتو تحدث كل يوم على الإنترنت، وأحيانًا ما تحدث عدة مرات في اليوم الواحد. وأصدقاؤنا في جمعية الإنترنت فعليًا يقومون بإعداد مرصد من أجل النظر في هذه الأحداث، وهم بصدد قياس 500-1,000 من هذه الأحدث كل عام على حدة. وقد كانت مستمرة منذ فترة تسعينيات القرن العشرين. وهذا ليس شيئًا جديدًا. والبعض منها ضار. البعض من هذا موجه لشخص يرغب في إحداث أذى لسبب ما. والكثير منها عرضي لأنه وعلى مدار العديد والعديد من السنوات، فإن المهندسين القائمين على بناء الإنترنت في حقيقة الأمر قاموا

بكتابة التكوينات يدويًا في أجهزة التوجيه. ونحن بشر، ونرتكب أخطاء إملائية. كما أننا نقترف أخطاءً. وعندما تقترف خطأً في جهاز توجيه، فقد يكون ذلك سيئًا. إن البنية التحية العامة الأساسية RPKI مصممة من أجل المساعدة في الكثير من تلك المشكلات، ولكن على وجه الخصوص ذلك السيناريو، وعلى وجه الخصوص سوء التكوين البشري. والبنية التحتية العامة الأساسية RPKI تساعد كثيرًا.

وما يعجبني في البنية التحية العامة الأساسية RPKI هو أنها لا تتطلب من كل جهاز توجيه يتحدث لغة بروتوكول البوابة الحدودية BGP أن يقوم بتوثيق الإعلانات. وقد تبين في نهاية المطاف أنه تتطلب فقط في حقيقة الأمر أن تقوم شبكات النقل الكبر في العالم بذلك لأنه، وعندما نقوم بمشاركة معلومات التوجيه من وزارتكم أو من مزود خدمة الإنترنت الخاص بكم، إلى هنا في شبكة اجتماع ICANN هنا في كانكون إلى فيسبوك في كاليفورنيا إلى شيء ما في فينزويلا أو شيء ما، فإن جميع تلك الحزم سوف تم بشكل نموذجي من خلال عدد بسيط للغاية—حوالي 800 أو نحو ذلك—كبار موفري الإنترنت ممن يوفرون النقل من أجل هذه الحزم. وقد تبين أن في حال كان هؤلاء الموفرين البالغ عددهم 800 أو نحو ذلك يوثقون ويوقعون المسارات، فإن كل شيء مما هو ليس صحيحًا ينخفض هناك، ولا يصل مرور البيانات إلى حيث يفترض أن يصل.

إذن من بين قصص النجاح الذي حققته البنية التحية العامة الأساسية RPKI والتوجيه الآمن بشكل عام على مدار السنوات القليلة الماضية هو 100% من الاعتماد لعدد 800 أو نحو ذلك من موفري خدمة الإنترنت في العالم في توثيق الحزم، وهو ما يعني أنه في حالة تشغيل شبكة أو في حالة تنظيم سلسلة من الشبكات، من الضروري جدًا أن تصدر تلك الشبكات الشهادات، وأيضًا ROA (تراخيص مصدر المسار) من أجل سوابق التوجيه لضمان قدر كل شيء على توثيق ذلك.

ولتأمين القناة بالكامل، ولتأمين الاتصالات بالكامل، فإننا بحاجة فقط إلى الحصول على البنية التحية العامة الأساسية RPKI. ويتعين علينا أيضًا توثيق المسار. فأي حزمة عندما تغادر جهازك وتنتقل إلى وجهتها وبعد ذلك تعود مرة أخرى، فإنها تمر بسلسلة من الشبكات الوسيطة، ويتوجب علينا التأكد من توثيق ذلك المسار طوال الوقت بحيث إن—ما نطلق عليه اسم هجوم الرجل الوسيط—شخص ما لا يمكنه تناول تلك الحزمة والبدء في التعامل معها عندما لا نقوم بالترخيص لهم بالقيام بذلك.

ولدى فريق عمل هندسة الإنترنت IETF بعض الحلول. فما زلنا نواصل التطوير والعمل للوصول إلى أفضل الحلول التي يمكن للجميع تنفيذها. وسوف يكون ذلك هو المرحلة التالية في رحلتنا للأمن في عالم أمن التوجيه.

سيرانوش فاردانيان: شكرًا.

ديفيد، هل يمكنك الانطلاق إلى ... وبعد ذلك نيكولاس. أنا أعرف أن لديك سؤالاً حول هيئة الإنترنت للأرقام المخصصة IANA.

ديفيد موندراغون: مرحبًا بكم جميعًا. أنا دانيال من مركز معلومات الشبكة بكوستاريكا وأهم مهندسًا كبيرًا للشبكات. ويتحمل مركز معلومات الشبكة في كوستاريكا المسئولية عن نطاقات المستوى الأعلى TLD في كوستا ريكا. لدي سؤالان. السؤال الأولى وهو؛ هل تبذل ICANN أو IANA أية جهود من أجل إنفاذ السياسات أو التقنيات من أجل استخدام نظام أسماء النطاقات DNS أو أمان طبقة النقل TLS بدلاً من DNS عبر HTTPS؟ لأن ذلك قد يمثل مشكلة بالنسبة لغالبية مهندسي الشبكات.

أما السؤال الثاني فهو، هي وجهة نظر هيئة الإنترنت للأرقام المخصصة وICANN حيال هذه المشكلة من منظور التوجيه والأمن السياسي؟

جون كرين: إذن الأول سهل. والإجابة لا لأنه لا يقع ضمن اختصاصنا. ونحن ندرس هذه الأشياء. ونقوم بقياسها. ونحن مهتمون بها. وهناك الكثير من النقاش في نواح أخرى حول الجهود المبذولة في ذلك. وإذا كنتم تقومون بأعمال البحث وكنتم تنظرون في حزم DNS وترغبون في الدخول إلى الحزم، فمن الواضح أنه لا يمكنكم القيام بذلك بموجب [الإبلاغ عن نشاط انتهاك النطاق DAAR] وأشياء من هذا القبيل. ويمكنكم إجراء عملية نقاشية في ذلك. هل هذا جيد؟ هل هذا سيء؟ أنا لا أعرف الإجابة، ومن ثم فإنني أتحدث فقط من منظور شخصي لأن هناك دائمًا احتقان فيما بين الأمن والخصوصية في هذا النوع من التقنيات.

ولا أدري إن كان لدينا موقف رسمي خاص حول حل نظام أسماء النطاقات عبر بروتوكول نقل النص التشعبي الآمن DoH. وقد أجرينا بعض الأبحاث حول ذلك.

ولأن مات لم يتحدث كثيرًا اليوم، وأنا أود التعرف على ما إن كان مستيقظا ويريد التحدث حول هذا أم لا.

مات لارسون: نعم، أنا كذلك. أنا مستيقظ هنا. نعم، لقد قمنا ببعض الأبحاث حول DNS عبر HTTP وDNS عبر أمان طبقة النقل TLS. وفي حقيقة الأمر، فقد أسهم بول هوفمان من فريق البحث في هذه الجهود من منظور المعايير. ومن ثم فقد ساعدنا في حقيقة الأمر في تطوير تلك المعايير.

وبالنظر إلى المصالح الإجمالية المتزايدة، أود القول بأنه في جانب الخصوصية، أعتقد أنه من الحتمي أننا سوف نرى المزيد والمزيد من نشر واستخدام هذه البروتوكولات.

وفي الوقت نفسه على الرغم من ذلك، فإنها أكثر كثافة من حيث الأعمال المحاسبية وأكثر كثافة من ناحية الشبكات لأن نظام أسماء النطاقات العادي ما هو إلى شبكة واحدة بالنسبة لأي استعلام وحزمة واحدة من أجل الاستجابة. وربما يحدث ذلك عبر اتصال TCP، وفي تلك الحالة توجد بضع حزم يتم تبادلها من أجل إعداد وتقسيم ذلك الاتصال.

لكن بمجرد بدء الحديث حول إضافة التشفير إلى ذلك، فإنك تتحدث حول التفاعلات المعقدة بشكل متزايد مع المزيد من الحزم. وموفرو الخدمات الذي يردون على الكثير من استعلامات DNS، مثل مشغلي TLD ومشغلي خادم الجذر متوترين قليلاً حيال ما يعنيه ذلك بالنسبة لبنيتهم التحتية. وإذا حدث أن جاء كل استعلام فجأة في غير حزمة واحدة عبر بروتوكول مخطط المستخدم UDP ولكن عوضًا عن ذلك يتطلب إعداد اتصال وحدوث توثيق تشفيري، فإن هذا الأمر مكثف أكثر. ومن ثم فإن من يقومون بإدارة وتشغيل البنية التحتية الحيوية على نطاق كبير لديهم مخاوف وأسئلة حيال ذلك.

لكنني أعتقد أنه من باعتبارنا صناعة ومجتمعًا، فإن هذا هو المكان الذي نلجأ إليه. ومن ثم أعتقد أنه من الحتمي أن نرى نشرًا وانتشارًا متزايدًا لتلك البروتوكولات.

سيرانوش فاردانيان: شكرًا.

أعتذر منك دانيال. لقد ناديتك ديفيد.

نيكولاس؟ سوف نتناول سؤالاً إضافيًا من نيكولاس، وبعد ذلك ديفيد سوف يعرض علينا جميعًا برنامج مبادرة تبادل المعرفة ومعايير التمثيل لنظام أسماء النطاقات وأمن التسمية. شكرًا.

نيكولاس فيوماريلي: شكرًا. لقد شاركت افتراضيًا عبر الإنترنت في الأسبوع الأخير من عملية مفتاح توقيع شفرة الدخول الأساسية، أعتقد ذلك. وهذا سؤال مرتبط بذلك لكنه مرتبط أيضًا [يتعذر تمييز الصوت] الامتدادات الأمنية لنظام أسماء النطاقات. هل هناك أية جهود متواصلة داخل فريق عمل هندسة الإنترنت من أجل تضمين التشفير ما بعد الكم في بروتوكول الامتدادات الأمنية لنظام أسماء النطاقات، وعلى وجه الخصوص فيما يتعلق بإدارة منطقة الجذر؟ وبالنظر إلى أنه كانت هناك بالفعل جهود لتضمين خوارزميات ما بعد الكم في البروتوكولات الأخرى في فريق عمل هندسة الإنترنت، فما هي التحديات التي يتوقعها فريق عمل هيئة المُعرّفات الفنية العامة في تنفيذ هذه الخوارزميات الجديدة داخل الامتدادات الأمنية لنظام أسماء النطاقات، وكيفي تخططون للتعامل مع هذه التحديات لأمن واستقرار نظام أسماء النطاقات؟ شكرًا.

كيم ديفيز: شكرًا لك على هذا السؤال. فبداية من الوقت الحالي، ليست لدينا أية مبادرات لتشفير ما بعد الكم من ضمن أهدافنا في الوقت الحالي، لكننا نجري بعض الأعمال التحضيرية من أجل تغيير خوارزمية التشفير في منطقة الجذر. لذلك فإننا نستخدم اليوم RSA-SHA256. ولم نقم من قبل في حقيقة الأمر بتغيير تلك الخوارزمية. ومن غير الواضح إن كان تغيير الخوارزمية سوف يكون صعبًا أو سهلاً. ومن ثم فقد قمنا في حقيقة الأمر بتشكيل فريق تصميم من المجتمع فقط في الأسابيع القليلة الماضية. وسوف يجتمعون في غضون أسبوعين في يوكوهاما من أجل الحديث حول هذا الأمر باستفاضة. وفي حقيقة الأمر فإن الغرض من هذا الفريق الخاص بالتصميم يتمثل في العمل على حل كيفية تغيير الخوارزمية في منطقة الجذر، سوف كان ذلك بالتشفير ما بعد الكم أو ربما كان ذلك شيء آخر مثل خوارزمية تشفير المنحنى البيضاوي والتي سوف تثمر عن أحجام أقل في الحزم [وأيضًا] نتائج أخرى مفيدة.

ومن ثم فإننا في تلك المرحلة حقًا. وأعتقد أن من السابق لأوانه البدء في التفكير حيال التشفير ما بعد الكم. وهذا بالتأكيد، أود القول، على نطاق واسع ضمن اهتماماتنا.

لكن من حيث طبيعة النشاط الجاري في تلك المساحة، فربما سوف أحيل الكلمة إلى مات من أجل الحديث حول أنشطة الأبحاث لأنني من حيث أجلس في الوقت الحالي بالتأكيد وعلى المستوى التشغيلي، أعتقد أن تشفير ما بعد الكم يتعلق أكثر بالأنشطة البحثية في الوقت الحالي.

مات لارسون: شكرًا لك، كيم. شكرًا لك على هذا السؤال. إذن هذه فرصة بالنسبة لي في الرجوع إلى سلسلة وثائق مكتب المسئول الفني الأول OCTO التي أشار إليها جون منذ عدة سنوات. ومن ثم فإن لدينا بالفعل وثيقة مكتوبة حول ذلك. وأنا لست في برنامج Zoom Room، ومن ثم لا يمكنني لصف الرابط، ولكنه يطلق عليه اسم OCTO-031: الحوسبة الكمومية وDNS. وهي فعليًا حول هذا الموضوع. ولأن التشفير ما بعد الكم يحظى بمزيد من الاهتمام، فقد أطلب مكتب المسئول الفني الأول برنامجًا للبحث التشفيري—وشائع للغاية—من أجل إجراء الأبحاث في مجال ما بعد الكم وكتابة ورقة بحثية حول ذلك. إذن فهي ورقة بحثية مقروءة لكنها مكثفة. ولكننا أجرينا إصدارًا عامًا أكثر في ذلك، ألا وهو OCTO-031. وهذا ما يعطي رأينا حول حالة الصناعة وما يجب علينا القلق حياله بالنسبة للتشفير ما بعد الكم. وأعتقد أن الإجابة هي: نحن بعيدون للغاية عن الاحتياج للقلق حيال خوارزميات ما بعد الكم لأننا بعيدون للغاية عن أجهزة كمبيوتر الكم والذي يمكن أن تكون له القدرة حتى على تشكيل تهديد للخوارزميات التي نستخدمها من أجل تشفير المفتاح العام اليوم.

ومن ثم أعتقد أن هذا مثال ذلك حيث يوجد الكثير من الغض في الصناعة والناس يتحدثون حول ذلك. والمعنى الذي يمكنكم الحصول عليه من ذلك هو قراءة المنشورات التجارية، "يا للخطأ! هذا أمر وشيك، والعالم ينهار، ويجب علينا أن نكون جميعًا على استعداد!" ولا يعني ذلك أنه لا يجب أن نكون على استعداد، لكن أمامنا أعوام إن لم يكن عقود. إذن في حقيقة الأمر فإن هذا هو موقفنا: ما يزال الوقت مبكرًا للغاية للبحث في الأمر. ما يزال لدينا الكثير من الوقت حتى الآن إلى الحصول على كمبيوتر الكم الذي يمكن أن يمثل تهديدًا لتشفير اليوم.

سيرانوش فاردانيان: شكرًا لك، مات. لقد تم نشر الرابط في مربع الدردشة في مساحة برنامج زووم. ومن ثم تفتحونه وتقرأون التفاصيل الواردة في المستند.

وفي الوقت ذاته، أود أو أعطي الكلمة إلى ديفيد من أجل الحديث حول مشروع مبادرة تبادل المعرفة ومعايير التمثيل لنظام أسماء النطاقات وأمن التسمية، رجاءً.

ديفيد هوبرمان: شكرًا لك، سيرانوش. إذن فقد أردت تغيير الموضوع بالنسبة للدقائق القليلة الأخرى المتبقية لدينا اليوم، وأردت أن أخبركم بشيء نقوم به في ICANN في محاولة لتحسين الوضع الفني للإنترنت؟.

لقد ذهبت للعشاء بالخارج ليلة أمس. وقد ذهبت إلى مطعم مع أحد الأصدقاء وأمضيت وقتًا رائعًا حقًا. وخلال تقديم طعام العشاء إلينا، قام الساقي بشيء أعتقد أنه سيناريو كارثي بالنسبة للساقي. فقد أراق المشروب الخاص بي فوق تمامًا أثناء إعادة ملء الكوب، مما تسبب في بلل كل ملابسي. وعندما حدث ذلك، فإن هناك طريقتان أو ثلاث طرق يمكننا نحن البشر الاستجابة لذلك من خلالها. قد نصاب بالغضب جميعًا ونقول "ما هذا؟! ما الذي تفعله؟!" وتكون هناك ثورة غضب، والأمر يكون صعبًا ومحرجًا للجميع. ويمكن أن نجلس هناك بلا حراك وبدون ردة فعل. أو يمكننا اتخاذ الأسلوب الامثل، وهو أنه يمكننا الضحك ويمكننا الابتسام كما يمكننا القول، "لا بأس. لقد أخطأت. لا داعي للقلق يا صاح". ويمكننا أن نتعرض لموقف سيء ونجعله جيدًا.

حسنًا، إذن فقد قمنا بذلك في الليلة الماضي، وكان الساقي على ما يرام، وضحكنا، وأصبحنا أصدقاء، ولم يكن الأمر يستدعي كل ذلك. لا بأس. لماذا أتحدث عن هذا الأمر؟ لأنه يمكننا القيام بنفس الشيء في نظام أسماء النطاقات DNS. يمكننا التحلي بالكياسة، ويمكننا جعل الحياة أفضل بالنسبة للجميع من خلال اتخاذ بعض الإجراءات المحددة، والإجراء المصغرة من اللطف تجاه بعضنا بعضًا.

لقد أنشأت ICANN برنامجًا يطلق عليه مبادرة تبادل المعرفة ومعايير التمثيل لنظام أسماء النطاقات وأمن التسمية KINDNS. وهو عبارة عن موقع على الويب، KINDNS.org. والغرض من المبادرة بالنسبة لجميع مشغلي نظام أسماء النطاقات، الكبار والصغار، سواء كنت شركة Google أو شركة فيسبوك، وسواء كنت مزود خدمة إنترنت جديدًا في مقدونيا ... أيًا ما كنت،

فهناك خطوات يمكنك اتخاذها بصفتك مشغل DNS لكي تكون أكثر لطفًا. وإذا كان الجميع أكثر لطفًا، فإن نظام أسماء النطاقات DNS نفسه يمكن أن يحظى بوضع فني قوي ومحسن.

لذلك في هذا المشروع، فإنه يتم تصنيفك حسب نوع المشغل الذي أنت عليه بالفعل. فأنت تدير وحدة حل التصديق تكرارية صغيرة وخاصة. وتدير خادمًا رسميًا يعطي ردودًا على أسماء وأسئلة DNS. أو بما كنت وحدة حل تصديق عامة وتريد من جميع من في العالم أن يكونوا قادرين على استخدامها. ومن خلال مشروع مبادرة تبادل المعرفة ومعايير التمثيل لنظام أسماء النطاقات وأمن التسمية، يمكنك أخذ تقييم ذاتي بصفتك مشغل ومعرفة مستوى أدائك، والحكم عليك في مقابل مجموعة من المعايير التي يضعها المجتمع—ICANN ومجتمع DNS الفني—واتفق عليها والتي تعد مجموعة من المعايير الأساسية التي يجب على الجميع الالتزام بها، وإذا ما التزم الجميع بها، فمن المرجح أن يعمل نظام أسماء النطاقات DNS بشكل أفضل. وسوف يكون أكثر أمانًا وأكثر استقرارًا. ويمكنك الاختبار في مقابل هذه المجموعة من المعايير ومعرفة مستوى أدائك، والحصول على نتيجة خاصة للتأكد مما وصلت إليه، وهل كانت هناك فجوات أم لا، وتكون لديك الفرصة لسد تلك الفجوات.

وهذه من الجهود التي تمت نمذجتها من واقع شيء ما، وهو من الأشياء التي قما بها زملاؤنا في جمعية الإنترنت في مجال أمن توجيه مسار البيانات. وهم يطلقون عليها اسم التحلي بالذوق والأخلاق العامة. ونحن نطلق عليها التحلي باللطف. ومن خلال هذه الأنواع من المبادرات، يمكن للمجتمع بالكامل العمل على تحسين جودة الأشياء أمام الجميع والقيام بذلك من خلال سلسلة صغيرة جدًا من الخطوات التي لا تكلف مالاً، في المعتاد، ولا تستهلك هذا القدر الهائل من الوقت. بل إنها تساعد فقط على فهم المكان الذي وصلت إليه شبكتك وإجراء تغييرات بسيطة من أجل تحسين تلك الشبكة وتحسين البيئة التحتية لنظام أسماء النطاقات بحيث يمكن للجميع تحقيق الاستفادة.

إذن هذا هو المقصود بمبادرة تبادل المعرفة ومعايير التمثيل لنظام أسماء النطاقات وأمن التسمية KINDNS. لذلك إذا سنحت لك فرصة، عندما يكون لديك متسع من الوقت، أن تلقي نظرة على موقع KINDNS.org على الويب. وسوف ترى هناك بصياغة بسيطة للغاية بعضًا من المعايير المقبولة لدى المجتمع والتي نعتمد أن على الجميع الالتزام بها.

وهذا كل ما أردت مشاركته معكم. شكرًا.

سيرانوش فاردانيان: شكرًا لك، ديفيد.

لدينا سؤال من مشارك عن بعد من محمد النور عبد الحافظ فضل من جمعية الإنترنت بالسودان. "توثيق المسار أمر ضروري وهام بالنسبة لأمن طاولة التوجيه العالمي. تم طرح امتداد BGPsec للتخلص من هذه المشكلة، لكنه يواجه صعوبات فيما يخص إمكانية نشره واستخدامه بسبب الموارد الضخمة التي يستهلكها BGPsec. ويلزم إجراء أبحاث من أجل تحسين مستوى الامتداد وجعله أكثر قدرة على النشر والاستخدام. ما دور ICANN في هذه المسألة؟"

جون كرين: ثمة دوران إلى حد ما يمكننا تأديتهما هنا. الأول بالطبع وهو المشاركة، والثاني بالطبع وهو المشاركة في الأبحاث.

ومن ثم أعتقد أنني سوف أحيل الكلمة إلى ديفيد. هل تريد تناول هذا السؤال؟

ديفيد هوبرمان: إنه سؤال رائع. شكرًا. كما كنت أقول دائمًا من قبل، فإن مسارا الوصول إلى بنية تحتية للتوجيه الآمن هما البنية التحية العامة الأساسية RPKI وتوثيق المسار. وكما يوضع السؤال من طرف خفي، فإن لدينا بالفعل حل لذلك. لقد قام فريق عمل هندسة الإنترنت بالفعل بوضع حل يطلق عليه اسم BGPsec—أو أمن BGP افتراضًا، اتفقنا؟ لكن وكما يشير صديقنا، فإن نشر BGPsec أمر غير واقعي تمامًا في الوقت الحالي لأن النفقات المحاسبية لأي جهاز توجيه هائلة للغاية ... ولن نقوم بتقسيم الإنترنت. لا، فسوف نقوم بعمل أكثر سوءًا بكثير. سوف نؤدي إلى إبطاء سرعته.

إذن بالنسبة لـ ICANN، فإن مشاركتنا في الأبحاث والمشاركة في الحلول الأخرى، في جانب منه هو ما سيقوم به فريق مات وفرق العمل الأخرى في ICANN من حيث المشاركة في عمليات وضع معايير البروتوكولات—وأنا أشير على وجه التحديد إلى فريق عمل هندسة الإنترنت هنا. فعندما تخرج إلينا الحلول فيمكننا بالطبع قياس تأثير تلك الحلول. ويمكننا قياسها من الناحية الرسمية والعلمية. ويمكننا إجراء قياس قائم على الملاحظة لها من خلال ملاحظاتنا ومن خلال

تفاعلاتنا مع أعضاء المجتمع. ويمكننا أيضًا بعد ذلك العمل كقائمين على تسهيل المناقشات وعلى وجه الخصوص التركيز أكثر في مجتمع ICANN مع الأسماء والأرقام، من أجل التعرف على التأثيرات، ومعرفة البواعث، والتحقق من المحفزات حول الطريقة التي يمكن أن تؤدي بها هذه التقنيات إلى تحسين (أو لا) الموقف على الأرض.

جون كرين: حسنًا، شكرًا لك، ديفيد.

أنا أتساءل، كم عدد الأشخاص في القاعة قاموا فعليًا من قبل المشاركة في فريق عمل هندسة الإنترنت؟

هذا جيد. ثمة عدد قليل منكم. إذا كنت مختصًا في مجال التكنولوجيا وكنت مهتمًا بالبروتوكولات، فهذا هو المكان المناسب لك. وإذا لم تكون شغوفًا بالتكنولوجيا، فسوف تصاب بالارتباك عند الوصول إلى هناك. لكن بالنسبة للمهووسين بالتكنولوجيا من بيننا، فإن فريق عمل هندسة الإنترنت هي المكان المناسب لكم فعليًا.

ومن المهم أن نتذكر ذلك—سوف تصاب بالدهشة عند سماع ذلك—ICANN لا تدير الإنترنت. وICANN لا تقوم على تطوير الإنترنت. ولا نقوم بتطوير جميع البروتوكولات. فهذه شراكة. وهي عبارة عن مجتمع من المهندسين والأشخاص الذين يستخدمون الإنترنت ممن يقومون فعليًا بذلك. لذلك من الرائع رؤية أشخاص في فريق عمل هندسة الإنترنت ومنتديات أخرى وليس فقط هنا.

أعتقد أننا انتهينا عند هذا القدر؟ أم هل لدينا المزيد من الأسئلة؟

سيرانوش فاردانيان: يمكنني أخذ سؤال واحد أخير.

نعم، رجاءً؟ عفيفة، ، هل إنني أراك؟

نعم. عفيفة، تفضلي.

عفيفة عباس: مرحبًا بكم جميعًا. أنا عفيفة. وأنا أحد مرشدات الزمالة. وقد مر عامان على بداية عملي في إرشاد الزملاء. إذن لدي سؤال واحد يتم طرحه عليّ مرارًا من الزملاء وهو، أين ICANN من حيث الوافدين الجدد إلى عالم أمن الفضاء الإلكتروني، هل يمكن إشراكهم، حيث يمكنهم القول بكل فخر أنهم ينتمون إلى هذا أمن الفضاء الإلكتروني على وجه الخصوص في ICANN. إذن من خلال العمل مرشدًا، فقد واجهت صعوبات في الرد على هذا السؤال لأنه ... إذن هلال تكرمتم بتسمية بضع منصات بحيث يمكننا المشاركة فيها. لأنني وبصفتي مرشدة، يمكنني القول بأن هناك مجموعة كبيرة قادمة وهم مهتمون للغاية بأمن الفضاء الإلكتروني. وكما قلتم، فإن زمالة ICANN تقوم بالأساس على ضخ دماء جديدة فيها. ولا نريد خسارة هذه المجموعة، وأنا أيضًا على يقين من أن ICANN لا تريد هذا هي الأخرى. إذن كيف يمكننا استغلال هذه الموهبة من حيث أمن الفضاء الإلكتروني؟ شكرًا.

جون كرين: حسنًا، شكرًا لك، عفيفة. ومرحبًا. من الممتع دومًا أن نرى زملاء يعاودون المشاركة، وعلى وجه الخصوص عندما يتحولون إلى مرشدين. هذا رائع. إذن هذا سؤال شيق لأن ICANN ليست منتدى معنيًا بأمن الفضاء الإلكتروني، اتفقنا؟ فليست هذه هي مهمتنا. لكن لدينا مسار خاص بالأمن حيث تكون الأشياء [يتعذر تمييز الصوت] في ذلك المسار داخل جدول أعمال ICANN.

إذا كنتم تبحثون عن النصيحة حول المكان الذي يجب عليكم المشاركة فيه من أجل مشكلات أمن الفضاء الإلكتروني داخل ICANN الآن، فإن لدينا لجنة يطلق عليها SSAC (اللجنة الاستشارية للأمن والاستقرار). ويمكنكم التقدم من أجل الالتحاق بعضويتها. فهم يبحثون عن المتخصصين الأكثر خبرة في مكان الأمن هناك. فإذا كنت قادمًا بصفتك زميلاً، أو متخصصًا مخضرمًا في مجال الأمن—لأنه ولعلكم تعلمون لدينا أشخاص كانوا في الصناعة لمدة بصفة زملاء—فهذا هو المكان الذي يجب عليكم التطلع إليه.

ولدينا أيام مخصصة للجوانب الفنية. كما أن منظمة دعم أسماء رموز البلدان ccNSO تعقد سلسلة من الأيام المخصصة للجوانب الفنية تُجرى فيها العديد من الجلسات المعنية بموضوع الأمن.

وبالطبع يمكنكم دائمًا المجيء إلينا ويمكننا مساعدتكم في العثور على الجوانب والأشخاص الآخرين من أجل التحدث إليهم.

والكثير مما هو مهم في ICANN ليس فقط ما يحدث في مناقشات السياسات. ولا تنسوا أن ICANN هي عبارة عن منتدى لمناقشة السياسات. ولكنها حول السياسات الخاصة بالمعرّفات، وهي لا تختص فقط بالأمن وبالتأكيد ليس فقط بأمن الفضاء الإلكتروني. لكن الأمر الهام الذي تقومون به هنا هو التفاعل مع الناس في الأروقة وفي الفعاليات.

إذن إذا ما رأيتم شخصًا وتريدون الاجتماع به—لا أدري—وهو في مجالكم، سواء كان ذلك أمن الفضاء الإلكتروني أو أي مجال آخر—فلا تترددوا في التحدث إلى مرشديكم أو الانطلاق للبحث عن أحد أعضاء فريق عمل ICANN أو أي شخص بصراحة في المجتمع والقول له، "مرحبًا، أنا مهتم فعليًا بالموضع س، وقد رأيت أن هذا الشخص هو في الحقيقة الأعلم بهذا المجال. هل يمكنك تعريفي به؟" لأننا جميعًا سوف نفعل ذلك. وهذا الأمر يتعلق بالتعاون والعمل معًا، بشكل تصاعدي، ضمن مجتمع واحد. وللقيام بذلك، يجب علينا في حقيقة الأمر تشكيل مجتمعات.

فهذه إذن هي أفضل نصيحة يمكنني إسدائها لكم. وهناك مسار للأمن، لذا عليكم النظر في ذلك. انظروا إلى ccTLD، واليوم الفني. وتحدثوا إلى الأشخاص من اللجنة الاستشارية للأمن والاستقرار. وتحدثوا إلى أشخاص من لجنة RSSAC. وهي تعني اللجنة الاستشارية لنظام خادم الجذر. وإذا كنت من نطاقات ccTLD—هل هناك أي أحد من نطاقات ccTLD؟ أعرف أن هناك القليل. ارفعوا أيديكم.

هل تتعاملون في مجال الأمن؟

هل أنتم على قائمة أمن نطاقات ccTLD؟

وإذا كنتم مشتركين في منظمة دعم أسماء رموز البلدان ccNSO، فإن لديهم أيضًا مسائل تتعلق بالأمن.

وليست هناك إجابة مباشرة على ذلك، وهذا هو السبب في معاناتك في إخبارهم بذلك. [أرسلونا] إلى آخرين. وسوف نجري مناقشة وجهًا لوجه معكم ونرى إن كان بالإمكان فهم ومعرفة ما يناسبكم فعليًا. والمشكلة تتمثل في الآتي، لقد استخدمتم كلمة "أمن الفضاء الإلكتروني" وهي تعني الكثير من الأشياء بالنسبة لمختلف الأشخاص. لكن يسرنا أن نقدم لكم المساعدة.

وأعتقد أن سامانا تريد قول شيء أيضًا. تفضل.

ساماناتاج علي: ثمة نقطة واحدة أود إضافتها إلى ما قاله جون بالفعل وهي أنه سؤال شيق للغاية لأننا في بعض الأحيان نناقش هذا الأمر ولكن ليس بطريقة نظامية. كما كنا نحصل أيضًا على متدربين، بالإضافة إلى ... لقد قمنا بمشروعات—مشروعات أصغر أو أكبر. ولم نتحدث حول هذه المسألة على المستوى الداخلي، ولكننا ... على أية حال، وبصفتنا فرق عمل معنية بالأبحاث، فإن لدينا مشروعات ونريد بالفعل الترحيب بالأفكار أو العمليات الخارجية داخل المجموعات الخاصة بنا وخارجها. فإذا كان ما لديكم من متدربين مهتمين بالأبحاث وإجراء المشروعات، برجاء عدم التردد في إرسالهم إلينا، ويمكننا إجراء مناقشات ومعرفة أفضل الطرق الممكنة للمضي في ذلك.

سيرانوش فاردانيان: شكرًا جزيلاً.

وبهذا، أود أن أتوجه بالشكر لكل المتحدثين—مات وساماتا وديفيد وجون وكيم—على ما بذلوه من وقت. وأنا أعرف أن لديك جدول أعمال مكتظ للغاية، ولكنني أشكركم على بذل الوقت من أجل المجيء والتحدث إلينا، والشكر موصول إلى الزملاء وإلى المشاركين في برنامج NextGen. فهم شغوفون فعليًا بمعرفة المزيد.

وكل الحاضرين هنا والمشاركين معنا، فأنتم تعرفونهم الآن. فكلما رأيتموهم في الأروقة ووددتم طرح أية أسئلة عليهم، فلا تترددوا في التواصل معهم ومبادرتهم بالأسئلة.

وبختام هذه الجلسة، أود القول: كونوا لطفاء مع بعضكم بعضًا. شكرًا جزيلاً. وقد انتهى هذا الاجتماع. يمكننا غلق التسجيل الآن. شكرًا جزيلاً.

[نهاية التدوين النصي]