AR

ICANN85 مومباي | منتدى المجتمع – من الاستقرار إلى البقاء: دور ICANN في مستقبل مرونة الإنترنت
الاثنين، 9 مارس/أذار 2026 – 10:45 إلى 12:00 بتوقيت الهند

(KATHY SCHNITT)
كاثي شنيت

أهلًا وسهلًا بكم في "من الاستقرار إلى البقاء: دور مؤسسة ICANN في مستقبل مرونة الإنترنت". اسمي كاثي، وأنا مديرة المشاركة لهذه الجلسة. ويُرجى العلم بأن هذه الجلسة يجري تسجيلها، وتحكُمُها القواعد السلوكية الخاصة بالمشاركين من مجتمع ICANN، ومعايير السلوك المتوقعة في ICANN، وكذلك سياسة ICANN لمناهضة التحرش.

ستشمل الترجمة الفورية خلال هذه الجلسة اللغات الإنجليزية والفرنسية والإسبانية والصينية والعربية والروسية والهندية. ويرجى مراعاة الإرشادات التوجيهية التالية من أجل المشاركة في هذه الجلسة. كما سأقوم بنشرها أيضًا في مربع الدردشة للعلم والمعرفة.

هناك ثلاث طرق لطرح الأسئلة. إذا كنت حاضرًا شخصيًا، يُرجى التوجه إلى الميكروفون وانتظار دورك. وإذا كنت ستحضر افتراضيًا، فأرسل سؤالك عبر مربع الأسئلة والأجوبة. وسأقرأ هذا السؤال بصوت عالٍ، أو يمكنك رفع يدك للتحدث مباشرة. ببساطة انقر على أيقونة رفع اليد في أسفل الشاشة للانضمام إلى قائمة الانتظار وسنقوم بإلغاء كتم صوتك عندما يحين دورك.

سواء كنت حاضرًا شخصيًا أو عن بُعد، عندما يحين وقت التحدث، يرجى ذكر اسمك للتسجيل، واللغة التي ستتحدث بها إذا كنت تتحدث بلغة أخرى غير الإنجليزية، والتحدث بوضوح وبوتيرة معتدلة. سأترك الكلمة الآن لرام موهان.

(RAM MOHAN)
رام موهان

شكرًا. مرحبًا، وأهلًا وسهلًا بكم في هذه الجلسة العامة. اسمي رام موهان، وأنا رئيس اللجنة الاستشارية للأمن والاستقرار التابعة لمؤسسة ICANN.

إذا نظرت إلى شوارع مومباي، سترى مثالًا رائعًا على المرونة. هذه مدينة لا تتوقف عن الحركة أبدًا، ليس لأن كل إشارة مرور خضراء، ولكن لأنها تتمتع بقدرة مذهلة على تجاوز العقبات. والإنترنت ليس مختلفًا. لكن اليوم، لم يعد ضمان مرونة الإنترنت مسألة تتعلق

ملحوظة: مايلي هو ما تم الحصول عليه من تدوين ماورد في الملف الصوتي وتحويله الى ملف كتابي نصّي. ورغم أن تدوين النصوص يتمتع بدقة عالية، إلا إنه في بعض الحالات قد تكون غير مكتملة أو غير دقيقة بسبب المقاطع غير المسموعة والتصحيحات النحوية. تنشر هذه الملفات لتكون بمثابة مصادر مساعدة للملفات الصوتية الأصلية، ولكن ينبغي ألا تُعامل كما لو كانت سجلات رسمية.

بوصول الحزم إلى وجهتها. المسألة هي ما إذا كان نظام الثقة الذي ينقل هذه الحزم قادرًا على البقاء أمام العواصف العديدة التي تتجمع حاليًا على حدوده.

هذه ليست مجرد قصة تقنية. إنها قصة عن التبعيات الخفية، والطاقة، وموردي الخدمات السحابية، واللوائح العالمية التي نعتمد عليها ولكننا لا نتحكم بها. وبينما نتجه نحو عالم يحركه الذكاء الاصطناعي والاتصال الدائم، فإن فهم نقاط الضعف هذه هو الفرق بين إزعاج بسيط وإغلاق عالمي.

المرونة هي القدرة على الحفاظ على مصدر واحد للحقيقة حتى عندما يبدو العالم مجزأً. اليوم، لسنا هنا لمناقشة السياسة. نحن هنا لمناقشة الروابط التقنية، والبروتوكولات، والبنية التحتية، والاستقرار التشغيلي الذي يحافظ على ثبات المسار العالمي في ظل هبوب رياح التغيير.

نحن نتحدث عما إذا كانت الأنظمة التي يعتمد عليها مليارات الأشخاص يوميًا في الاتصالات والتجارة والخدمات العامة والأمن ستستمر في العمل في مواجهة الأعطال التقنية والتوترات الجيوسياسية والهجمات المتطورة بشكل متزايد.

لذا لدي هنا معي فريق من الخبراء المتميزين، وقبل أن نبدأ الجلسة، أود أن أشارك الجمهور أننا نخطط لاستخدام Mentimeter للتفاعل مع الجمهور طوال الجلسة. وما ستراه على الشاشة هو رمز الاستجابة السريعة. وعندما ترى رمز الاستجابة السريعة، أمسك هاتفك وامسح رمز الاستجابة السريعة وستظهر لك بعض الأسئلة.

نود أن نحصل على وجهة نظرك بشأن هذه الأسئلة وسنقدم لك المدخلات التي تقدمها لنا. وسنشارككم ذلك مع تقدمنا في المستقبل. انضم إليّ أنا وفيونا خمسة أعضاء في لجنة النقاش. داني ماكفرسون، يقود أقسام التكنولوجيا والأمن في VeriSign. شارك داني بنشاط في عمليات الإنترنت والبحث والتوحيد القياسي منذ أوائل التسعينيات، بما في ذلك العمل في مجلس هندسة الإنترنت ورئاسة مجموعة من فرق عمل هندسة الإنترنت وغيرها من مجموعات العمل واللجان. ولقد ألف العديد من الكتب والعديد من براءات الاختراع، ومعايير بروتوكول الإنترنت، ومنشورات أبحاث الشبكات والأمن.

وينضم إلينا أيضًا بروس تونكين، الرئيس التنفيذي لإدارة نطاق AU.، من AUDA. بروس يعمل هناك منذ عام 2017. قبل ذلك، أمضى 18 عامًا في معهد ملبورن للتكنولوجيا، الذي

كان أحد أول خمسة أمناء سجلات لدى ICANN. كما أمضى تسع سنوات ونصف في مجلس إدارة ICANN من عام 2007 إلى عام 2016، وكان رئيسًا للمنظمة الداعمة لاسم النطاق/المنظمة الداعمة للأسماء العامة لمدة خمس سنوات قبل ذلك.

وينضم إلينا أيضًا السيد ماكب سينغ. يشغل السيد سينغ حاليًا منصب كبير مسؤولي التكنولوجيا في CyberPeace، وهو عضو سابق وكبير مسؤولي أمن المعلومات في وزارة الطاقة في حكومة الهند. في ذلك المنصب، قاد السيد سينغ مبادرات رئيسية في مجال التحول الطاقي والأمن السيبراني حتى تقاعده. يتمتع بخبرة تزيد عن ثلاثة عقود في قطاع الطاقة في الهند، حيث قاد التحول نحو مصادر الطاقة غير الأحفورية، مثل الطاقة الشمسية وطاقة الرياح والطاقة الكهرومائية.

وينضم إلينا أيضًا دان يورك. دان هو المدير الأول لقسم الثقة والأمان عبر الإنترنت في جمعية الإنترنت، حيث يقود تطوير مركز الثقة والأمان عبر الإنترنت التابع لجمعية الإنترنت. وهو يشارك في المجتمعات التقنية، بما في ذلك IETF. وهنا في ICANN، كان دان عضوًا في اللجنة البرامج لورشة عمل ICANN حول DNSSEC والأمن منذ عام 2014.

وهو متواجد على الإنترنت منذ ثمانينيات القرن الماضي، وهو مؤلف للعديد من الكتب حول الشبكات والأمن وIPv6 وLinux. بصفته عضوًا في هيئة موظفي جمعية الإنترنت منذ عام 2011، فقد عمل في مجموعة واسعة من المبادرات، بما في ذلك مرونة الإنترنت، وإغلاق الإنترنت، وأمن نظام اسم النطاق، وبروتوكول الإنترنت الإصدار السادس، والأقمار الصناعية في المدار الأرضي المنخفض.

وأخيرًا، لدينا أيضًا في فريقنا بول فيكسي. قام بول فيكسي بتصميم وتنفيذ ونشر العديد من امتدادات بروتوكول نظام اسم النطاق والتطبيقات المستخدمة في جميع أنحاء الإنترنت اليوم، بما في ذلك التحديثات الديناميكية وسمعة الشبكة وبرنامج BIND مفتوح المصدر. هو عضو سابق في SSAC، ويعمل حاليًا في RSSAC. فيونا، هل ترغبين في أن تقدمي نفسكِ أيضًا؟

(FIONA ALEXANDER)
فيونا ألكسندر

أهلًا بالجميع، بالتأكيد. فيونا ألكسندر، أعمل مع Salt Point Strategies، ولكنني مشاركة منذ فترة طويلة في ICANN في العديد من المناصب من السنوات الماضية. يسعدني الانضمام إليكم من واشنطن العاصمة.

(RAM MOHAN)
رام موهان

شكرًا. لذا، فإن الأسس الأصلية للإنترنت، مثل DNS وIPv4 وBGP، لا تزال تُبقي مليارات الأشخاص متصلين بالإنترنت، ولكن البيئة التي تعمل فيها كل هذه البروتوكولات قد تغيرت تمامًا. نلاحظ، بتواتر متزايد، انقطاعات متسلسلة شديدة وواسعة النطاق في الإنترنت ناجمة عن أعطال في الأنظمة الخارجية الحيوية التي يعتمد عليها الإنترنت، مثل شبكات الطاقة والمنصات السحابية وسلاسل توريد البرامج المعقدة.

المشكلة ليست في هشاشة البروتوكول. يبدو أن المشكلة تكمن في الهشاشة البيئية. نحن عند نقطة تحول. ليس الهدف اليوم تقديم شرح لكيفية عمل الإنترنت. لسنا هنا أيضًا لمناقشة لوائح ICANN أو ولاية ICANN، ولكننا هنا لمناقشة ما يحدث عندما تتعطل الأنظمة الأساسية حول الإنترنت، وما يحدث عندما تتعطل تطبيقات المستخدم التي تعتمد على هذه الأنظمة الأساسية. فيونا.

(FIONA ALEXANDER)
فيونا ألكسندر

مرحبًا، شكرًا يا رام. أعتقد أننا أردنا تقديم بعض السياق لمحادثة اليوم. وقد شارك العديد منا، بمن فيهم رام ودان وداني وآخرون، على مدار العام ونصف العام الماضيين في جهد بذلته جمعية ماركوني لدراسة مرونة الإنترنت.

لقد أنشأوا مجلسًا استشاريًا لمرونة الإنترنت، وكان العديد منا أعضاء فيه. ثم عقدوا أيضًا سلسلة من الاجتماعات وورش العمل حيث نظروا في مجموعة من القضايا وحاولوا معرفة ما يجب علينا فعله وكيف نجعل مرونة الإنترنت نوعًا من القضايا الأساسية للمضي قدمًا.

في نوفمبر/تشرين الثاني 2025، عقدوا ورشة عمل ومنتدى. مثّلت هذه الاجتماعات تتويجًا لجهود تعاونية استمرت عامًا كاملًا لمعالجة نقاط الضعف الحرجة والبنية التحتية العالمية للإنترنت. استنادًا إلى اجتماع أولي في الأكاديميات الوطنية للعلوم هنا في واشنطن العاصمة، والعمل المستمر عبر الإنترنت من خلال مجموعتي عمل متخصصتين.

أولًا، فريق عمل رسم خرائط سلسلة التوريد لمرونة الإنترنت الذي شاركت فيه. وثانيًا، فريق عمل إشراك مزودي خدمات الحوسبة السحابية العملاقة الذي شارك فيه رام بشكل كبير. وقد قام كلا فريقي العمل بإعداد سلسلة من التقارير، وجمع كلا الاجتماعين قادة العمليات والتقنية والسياسات والحوكمة لترجمة الخبرات المتنوعة إلى استراتيجيات مرونة قابلة للتنفيذ.

إن أهم ما يمكن استخلاصه من هذا الجهد هو أنه يجب التعامل مع المرونة كمبدأ تصميم أساسي، وليس كاعتبار ثانوي. لذا، إذا نظرنا إلى مواضيع تقرير جمعية ماركوني، ونظرنا إلى نوع المواضيع التي ظهرت من اللجنة الاستشارية للأمن والاستقرار التابعة لـ ICANN وSAC132، الذي صدر في سبتمبر/أيلول 2025، والتي تبحث في كيفية اعتماد نظام اسم النطاق DNS على البرامج المجانية والمفتوحة المصدر. لدينا أربعة مواضيع محددة نريد أن تغطيها جلسة اليوم.

أولًا، أعطال شبكة الطاقة الرئيسية وما يعنيه ذلك بالنسبة للإنترنت، وانقطاعات الخدمة المتتالية الناتجة عن أعطال السحابة وواجهات برمجة التطبيقات، والتدخلات السياسية والتنظيمية التي يمكن أن يكون لها آثار على نظام اسم النطاق، سواء كانت غير مقصودة أو متعمدة، وهجمات سلسلة توريد البرامج على نطاق غير مسبوق.

في هذا السياق، نريد أن نمنح كل عضو من أعضاء اللجنة ثلاث دقائق لتقديم مداخلته الافتتاحية. وإذا أمكننا أن نطلب من أعضاء اللجنة التحدث، فيُرجى الالتزام بثلاث دقائق، فسيكون ذلك رائعًا. سنبدأ مع داني. داني، الكلمة لك.

(DANNY MCPHERSON)
داني ماكفرسون

حسنًا. شكرًا يا فيونا، وتحياتي للجميع. سأركز على البنية التحتية الأساسية للإنترنت، لكن هذه التعليقات تنطبق بالتساوي على جميع مجالات التهديد المنهجي التي حددتها فيونا.

لقد أثبتت البروتوكولات الأساسية التي تُمكّن الإنترنت، وبروتوكول بوابة الحدود للتوجيه بين النطاقات، ونظام اسم النطاق الذي يُمكّن الملاحة العالمية بشكل فعال، أنها قوية للغاية في مواجهة عدم الاستقرار. ومع ذلك، لم يتم تصميم هذه البروتوكولات في الأصل مع

وضع الأمن في الاعتبار، بل اعتمدت على الثقة الضمنية بين مجموعة صغيرة نسبيًا من المشغلين.

الآن، كما نعلم جميعًا، تغير العالم وتوسع مجتمع المشغلين بشكل كبير، وتم تحديث بروتوكولات الإنترنت الأساسية هذه وبنيتها التحتية الداعمة، وما زالت تُحدث، بتحسينات أمنية.

تتضمن بعض الأمثلة البنية التحتية العامة للموارد لتمكين نظام توجيه أكثر أمانًا بين النطاقات وDNSSEC لمصادقة أصل البيانات وحماية سلامتها. على الرغم من أن هذه كلها تطورات مهمة، إلا أنها توسع أيضًا نطاق التشغيل الذي يجب أن يظل موثوقًا به. ببساطة، كل تحسين أمني جديد يضيف تعقيدًا، ومع التعقيد تأتي أنماط فشل إضافية أو طرق لتعطل الأشياء.

لقد خلقنا، بطريقة ما، مفارقة المرونة. إن الآليات المصممة لحماية الإنترنت يمكن أن تُدخل في حد ذاتها تبعيات ومشاكل نظامية جديدة. ومع ذلك، فإن هذه التحسينات الأمنية تهدف إلى منع حدوث اضطرابات كارثية أكثر خبثًا، وتتطلب دراسة متأنية ودقة بالغة في التنفيذ والعمليات.

مع وجود بروتوكولات أساسية تدعم الأنظمة الحيوية، فإنك ترغب في تقليل التبعيات النظامية وتجنب الاعتمادات الدائرية، ولكن في بعض الأحيان تكون هذه التبعيات غير ضرورية. علاوة على ذلك، عندما تأخذ بروتوكولات لا مركزية بطبيعتها وتضيف تبعيات نظامية جديدة، حتى وإن كانت مترابطة بشكل ضعيف، يصبح من الضروري تصميم مخازن مؤقتة وحواجز تشغيلية لطبقات متعددة من النظام بحيث يتمكن النظام بشكل شامل من امتصاص الصدمات غير المتوقعة بدلًا من نشرها أو تسلسلها بشكل منهجي.

عندما أفكر في المصير المشترك والاستقرار، أفكر فيما أهتم به في نهاية المطاف؟ أين يعيش؟ ما الذي يُمكّن ذلك؟ وما هي ضوابط الأمان للأداء اللازمة لتشغيله وحمايته؟ وما هي المخاطر التي يجب التخفيف منها والمرتبطة بذلك؟ أو بعبارة أبسط، على ماذا أعتمد في نهاية المطاف؟

(KATHY SCHNITT)
كاثي شنيت

داني، آسف على المقاطعة. هل يمكنك من فضلك التخفيف من سرعتك قليلًا مراعاةً للمترجمين؟

(DANNY MCPHERSON)
داني ماكفرسون

نعم، معذرة. المعذرة. أجل، ليست هناك مشكلة. وماذا يعتمد عليّ؟ لذا، بالنسبة لعمليات البنية التحتية لنظام اسم النطاق، تشمل هذه الأشياء البنية التحتية للنقل الأساسية، والمكونات المختلفة لنظام التوجيه، والذي يشمل الآن البنية التحية الأساسية للمفتاح العام، وأجهزة الشبكة والكمبيوتر، وتنوع نظام التشغيل، وتنوع تطبيقات الخدمة، ومرونة الأنظمة وسرعتها، وأنظمة الهوية والوصول والتحكم الداعمة، وضوابط نقاط نهاية الشبكة والأمان.

مع ازدياد ترابط البنية التحتية وتركزها بشكل متزايد في بيئات متعددة المستأجرين كبيرة الحجم، يزداد أيضًا نصف قطر الانفجار المحتمل. إن وجود ثقافة أحادية للممارسات داخل الشركات العملاقة أو الشركات العملاقة في مجال الحوسبة السحابية أو شبكات توصيل المحتوى CDNs والاعتمادات المتعدية على الثقة في البرامج، والثقة المتعدية في بروتوكولات الشبكة والأمان، وما إلى ذلك، كلها تؤثر على حسابات المتانة هذه.

من الأهمية بمكان أن يقوم المشغلون بحصر هذه المخاطر وفهم نطاق هجومها، وأن يتم النظر بشكل صحيح في كل من تحليل التأثير والنتائج لسيناريوهات الفشل المختلفة ومعالجتها عند الاقتضاء، ويفضل أن يكون ذلك قبل حدوث حالات الفشل. هذا كل شيء. بياني الافتتاحي.

(FIONA ALEXANDER)
فيونا ألكسندر

شكرًا يا داني. المتحدث التالي لدينا هو بول فيكسي. بول، أعتقد أنك موجود هناك، على الشاشة مباشرة.

(PAUL VIXIE)
بول فيكسي

مرحبًا. هل يمكنكم سماعي؟

(FIONA ALEXANDER) نعم، تفضل.
فيونا ألكسندر

(RAM MOHAN) صوتك ضعيف قليلًا يا بول، لذا ربما عليك الاقتراب قليلًا من الميكروفون.
رام موهان

(PAUL VIXIE) حسنًا. سأفعل ما بوسعي. سأقوم بإيقاف تشغيل الفيديو الآن. لذا أود أن أتحدث قليلًا عن سلسلة توريد البرمجيات، وهو موضوع ذو أهمية دائمة. لم يكن من الممكن إنشاء الإنترنت إلا من خلال مجموعة كاملة من التبعيات غير التعاقدية. بمعنى آخر، كان يتم إنشاء البرامج والبروتوكولات في كل مكان من قبل الكثير من الأشخاص المهتمين برؤية الأشياء تعمل.
بول فيكسي

وعادةً لا يتم دفع أي مقابل إذا كنت تقوم بتطوير برامج ونشرها على الإنترنت ليقوم الآخرون بجلبها وتنزيلها. لم تكن تتوقع أن تحصل على أجر مقابل ذلك. كان دافعك شيئًا آخر. وما يعنيه ذلك هو أن مسألة التبعيات غير التعاقدية هذه قد استمرت حتى يومنا هذا.

أعتقد أننا جميعًا ندرك أن البرامج بها أخطاء، وأن جميع البرامج على مر التاريخ كانت بها أخطاء، وأننا نتوقع أن جميع البرامج ستظل بها أخطاء إلى الأبد. من المقلق تنزيل البرامج، سواء كانت مفتوحة المصدر أو ربما تطبيقًا لهاتفك، أيًا كان نوعها، مع العلم أنها تحتوي على أخطاء، ولكنك لا تعرف ماهيتها بعد. لكن التحديثات قادمة. أعتقد أن كل واحد منا يمتلك مجموعة من أجهزة الكمبيوتر المحمولة والهواتف الذكية، أو أي شيء آخر.

نتوقع أن يصل حجم تحديثات البرامج إلى حوالي غيغابايت واحد أسبوعيًا لتلك الأجهزة، وهذا في الغالب لإصلاح العيوب. هذا ليس توسيعًا، على الرغم من أننا لم نكن لنصل إلى هنا إلا بهذه الطريقة. من الواضح لنا جميعًا ممن يفكرون في هذه الأمور ويتحدثون عنها أننا سنضطر إلى إيجاد شيء أفضل، لأنه على نطاق واسع، ما يحدث هو أن مطور البرامج سيفهم وجود عيب جديد في عمله وسيقوم بإصلاحه.

ثم يتساءلون: هل هذا الأمر متعلق بالأمن؟ هل من الممكن أن يؤدي نشر هذا إلى إصابة الكثير من الأشخاص من قبل أشخاص آخرين، مهاجمين سيستخدمونه قبل أن يتم إصلاحه؟ وإذا كان الأمر كذلك، فكيف يمكنني نشر التحديث قبل أن يتمكن المهاجمون من الحصول عليه؟ هذه مشكلة كبيرة. وربما ترغب في إخبار هؤلاء الأشخاص بأن التحررية لها تأثير طويل الأمد على ثقافة الإنترنت، وقد تقول لهم ببساطة: انشروا برامجكم، ودعوا الناس يتأقلمون. لكن مهما كان الدافع الذي يدفعنا لإنشاء البرنامج في المقام الأول، فمن المحتمل أنه يحفزنا على الرغبة في أن يستخدمه الناس بأمان.

ولذلك، فإننا نبحث عن حلول، وأحيانًا حلول إبداعية، لكننا لا نفعل ذلك بسبب الطبيعة غير التعاقدية لهذه التبعيات. ليس لدينا قائمة بأسماء مستخدمي برنامجنا. وبالفعل، قد ينتشر البرنامج عبر مسارات غير مباشرة حيث يقوم بعض مُجمِّعي البرامج، أو بعض صانعي التطبيقات الآخرين، أو ربما صانعي أنظمة التشغيل، بتضمين برنامجنا داخل شيء آخر. وإذا كنا لا نعرف من هم، فمن المؤكد أننا لا نعرف من هم عملاؤهم النهائيون.

إذن، هذه مشكلة. فلننظر إلى هذا من الجانب الآخر. إذا كنت تعتمد على برامج مفتوحة المصدر، وأنا هنا لا أفكر في هاتفي الذكي أو حتى على جهاز الكمبيوتر المحمول الخاص بي، فنحن نفكر في سياق المؤسسة التقليدي حيث كنت بحاجة إلى شيء ما للقيام بالعمل الذي تقوم به الشركة. وأنت تعلم أن هناك بعض البرامج الجيدة حقًا.

(RAM MOHAN)
رام موهان

شكرًا لك، بول. أيها الحضور الكرام، حان الوقت لأخذ هواتفكم ومسح استطلاع الرأي هذا من Mentimeter. إجاباتك مجهولة الهوية. لا يحتفظ هذا التطبيق بأي بيانات. لكن ما عليك سوى أخذ هاتفك. ألقِ نظرة على السؤال بينما ننتقل إلى عضو اللجنة الثالث، السيد سينغ. أجل.

(SHRI M. A. K. P. SINGH)
شري ماكب سينغ

أنا شري ماكب سينغ. أنا كبير المسؤولين التقنيين في CyberPeace. لذا، وبما أنني من قطاع الطاقة، أود أن أربط بين البنية التحتية الرقمية وأمن الطاقة. إذن، نحن بحاجة

إلى الكهرباء لتشغيل أجهزة التوجيه، ونحن بحاجة إلى أجهزة التوجيه لتشغيل الشبكة. كلاهما مترابطان.

يُعد قطاع الطاقة من أهم القطاعات الحيوية. لدينا في الهند سبعة قطاعات حيوية. أما في الولايات المتحدة، فلديهم 16. إذا فشل قطاع الطاقة، فإنه يشل قطاعات أخرى. في الواقع، الانتقال من انقطاع التيار الكهربائي إلى انقطاع الاتصالات سريع للغاية.

لذا، سأعطيكم مثالًا على انقطاع التيار الكهربائي عام 2003 في الولايات المتحدة وكندا، لقد كان انقطاعًا يمكن السيطرة عليه، لكنه تسبب في انهيار جزء كبير من نظام الكهرباء الإقليمي في شمال شرق البلاد، وتعطلت أبراج الاتصالات، وتعطلت آلات تسجيل النقد، وتعطلت أجهزة الصراف الآلي، وتوقف نظام النقل العام في كليفلاند، وتوقفت المضخات الكهربائية في وحدة المياه.

لذا، هذا هو نوع التأثير الذي يحدث عند انقطاع التيار الكهربائي، وقد شهدنا العديد من هذه الحالات. ما يحدث بالضبط هو أن تأثير فشل الشبكة يتمثل في استنزاف البنية التحتية. أبراج الاتصالات ومراكز البيانات، لديهم مرفق احتياطي من بطاريات الرصاص الحمضية، وعادة ما يكون لديهم ما بين ساعتين إلى ثلاث أو أربع ساعات كحد أقصى للاحتياطي.

لذا، إذا لم تتم استعادة الطاقة، فلن تعمل هذه الأنظمة، وفي الواقع، فإن مراكز البيانات هذه والخوادم الموجودة هناك تستهلك الكثير من الطاقة. إنها تولد الحرارة، وفي حالة عدم وجود تبريد، فإنها تقوم بتنفيذ الإغلاق الطارئ لمنع الذوبان المادي للأنظمة، وإيقاف خدمات الحوسبة السحابية وتوجيه الإنترنت.

إذن، هذا هو التأثير المهم الذي يحدثه. أولًا، علاوة على ذلك، فإن الانهيار اللوجستي المطلوب لإعادة الطاقة نفسها معطل، مما يؤخر هذا الجهد لإعادة تشغيل الشبكة، في الواقع.

(KATHY SCHNITT) معذرةً، آسفة. هل يمكنك من فضلك التخفيف من السرعة مراعاةً للمترجمين؟

كاثي شنيت

(SHRI M. A. K. P. SINGH) حسنًا، شكرًا.
شري ماكب سينغ

(KATHY SCHNITT) شكرًا.
كاثي شنيت

(SHRI M. A. K. P. SINGH) كما هو الحال في أوكرانيا، عندما تم تنفيذ الهجوم الإلكتروني، قام المهاجمون بشن هجوم الحجب المنتشر للخدمة على الخطوط الأرضية، لذلك يمكن أن يحدث هذا النوع من التأثير في حادث مادي أيضًا. عندما حدث هذا، في عام 2012، عندما انقطع التيار الكهربائي في بلدنا في الهند، فرضنا أن يكون لكل منشأة في قطاع الطاقة هواتف تعمل بالأقمار الصناعية، وذلك لأنها مفيدة للغاية في حالة انقطاع التيار الكهربائي لإعادة تشغيل الشبكة والتواصل من أجل إعادة تشغيلها.
شري ماكب سينغ

لذا، بالانتقال إلى الجانب الآخر من الأمر، كما هو الحال عند حدوث عطل في الشبكة، فإن انقطاع التيار الكهربائي يحدث بالفعل. لذا، تعتمد محطات الطاقة على عُقد الاتصال للتحكم ومعدات الاتصال. يعتمدون على شبكة الكهرباء للحصول على الكهرباء. يمكن أن تتسبب الأعطال في جزء محدود من شبكة واحدة في حدوث سلسلة من الأعطال بين هاتين الشبكتين بنمط متعرج، مما يؤدي إلى أعطال واسعة النطاق حتى في الشبكات المتشابكة عالية الاتصال.

ما يحدث هو أن لدينا العديد من الأجهزة التي تعمل على الإنترنت، وعلى الرغم من أنها قد لا تكون إنترنت عامة، إلا أنها قد تكون إنترنت خاصة، مثل أجهزة إنترنت الأشياء IoT وإنترنت الأشياء الصناعية IIoT. إنها بمثابة عيون مشغل الشبكة لأنها تستشعر المعايير وتغذي SCADA، الذي يقوم مشغل الشبكة لدينا بتشغيل الشبكة عليه.

وفي حالة عدم وجود رؤية SCADA، فإننا نتابع المرافق البعيدة، ولكن في حالة فشل الشبكة، لا نستطيع تشغيل شبكاتنا عن بعد أيضًا. إذن، هذا هو السبب الأكبر لانقطاع التيار

الكهربائي في حالة تعطل الشبكة. في حالة انقطاع التيار الكهربائي في شمال شرق البلاد عام 2003، تحول عطل مادي محلي في جامعة أوكلاهوما إلى أزمة دولية ضخمة أثرت على 50 مليون شخص.

لذا، تتجه شركات المرافق في الوقت الحاضر بشكل متزايد إلى اعتماد شبكات SD-WAN لإدارة مسارات متعددة. لذا، لا بد من وجود قدر من المرونة. إذا تعطل أحد مسارات الاتصال بالإنترنت، فيجب أن تعمل مسارات أخرى لضمان استمرار عمل الطاقة. الكهرباء متوفرة، وستكون المرافق الأخرى المرتبطة بها متوفرة أيضًا.

أكبر مشكلة اليوم هي أن معظم المعدات الموجودة في شبكة قطاع الطاقة هي أنظمة قديمة لأنها صُممت لتبقى لأكثر من 35 عامًا، ولكن نطاقها الزمني للأمن السيبراني محدود للغاية. لذا، هناك خطر آخر يتعلق بالأمن السيبراني لأن لدينا عددًا كبيرًا من الأنظمة القديمة المدمجة مع معظم التقنيات الحديثة أيضًا.

إذن، فهم يمثلون الإنترنت ومترابطون، ولا يمكننا الاستمرار في تشغيل الشبكات بشكل أعمى. لذا، يجب الحفاظ على أمن بنيتنا التحتية الرقمية، وللحفاظ على أمن البنية التحتية الرقمية، نحتاج إلى استمرار إمدادات الطاقة، وهذا هو الأهم.

(FIONA ALEXANDER)
فيونا ألكسندر

شكرًا جزيلًا يا سيد سينغ. أعتقد أن المتحدث التالي هو بروس.

(BRUCE TONKIN)
بروس تونكين

شكرًا لك، فيونا. طُلب مني تقديم بعض وجهات النظر من منظور مشغل رمز البلد، وأنا أعمل مع نطاق au. لأستراليا. بالنسبة للعديد من الاقتصادات القائمة على المعلومات، يتم التعامل مع نظام اسم النطاق DNS ونظام التسمية الوطني بطريقة مشابهة ربما لوجود شركة طيران وطنية. لقد أصبح جزءًا أساسيًا من اقتصادنا المحلي وقدرتنا على القيام بالتجارة الدولية. وبدأ التعامل معها كبنية تحتية حيوية بنفس الطريقة التي يتم بها التعامل مع المياه والكهرباء وتوزيع الغذاء والاتصالات في البلاد.

هناك اتجاه بدأ في بعض الدول المتقدمة، بما في ذلك أستراليا، للبدء في سن قوانين تشريعية لتنظيم أنظمة اسم النطاق بنفس الطريقة التي توجد بها قوانين تتعلق بحماية أصول المياه أو الكهرباء. وبموجب التشريعات الأسترالية في au.، نحن مطالبون بأخذ ما يسمونه نهج إدارة المخاطر الشامل لجميع المخاطر.

وهذا يشمل أربعة مجالات رئيسية. الأمن السيبراني وأمن المعلومات، وكثيرًا ما نتحدث كثيرًا عن ذلك في اجتماعات ICANN، ولكن أيضًا عن مخاطر الموظفين. ويمكن أن يكون ذلك من خلال شخص يحاول بسوء نية القيام بشيء ما للبنية التحتية أو ببساطة خطأ بشري.

تُعتبر سلسلة التوريد بشكل متزايد مصدرًا للمخاطر، ثم تأتي المخاطر الناجمة عن الكوارث الطبيعية أو الفيزيائية. عندما تحدث الكوارث، سواء كانت طبيعية، والتي قد تكون ناجمة عن الحرائق أو الفيضانات أو الزلازل أو الأعاصير أو الأوبئة الشبيهة بكوفيد، أو من صنع الإنسان، سواء كانت نتيجة حرب أو نتيجة هجمات إلكترونية من منظمات إجرامية. عندما تحدث هذه الكوارث، فإنها تؤثر في الواقع على أجزاء متعددة من البنية التحتية الحيوية في نفس الوقت.

لذا، لن يؤثر ذلك على الكهرباء فقط أو على نظام اسم النطاق فقط، بل سيؤثر في الواقع على كليهما في نفس الوقت. لذا، هناك وعي متزايد بأن التبعيات بين صناعات البنية التحتية الحيوية لها تبعيات من حيث أننا قد نستخدم مزودي خدمات سحابية مشتركة.

لذا، من الممكن أن تستخدم كل من صناعة الكهرباء وصناعة نظام اسم النطاق خدمات أمازون السحابية Amazon Web Services في الخلفية. لذا، إذا تعطل مركز البيانات، كما ذكر السيد سينغ، فإنه سيؤدي إلى تعطيل كل من نظام اسم النطاق وشبكة الكهرباء. هناك أيضًا استخدام كبير، وأعتقد أن بول كان يشير إلى هذا، لكننا نستخدم برامج مشتركة. وكانت دراسة حالة ذلك مؤخرًا هي العام الماضي مع CrowdStrike. وقد أثر ذلك على أجزاء متعددة من البنية التحتية الحيوية في نفس الوقت.

لذا، هناك وعي بأننا بحاجة إلى النظر في سلسلة التوريد بأكملها، سواء من حيث الأمن السيبراني، أو من حيث الترابطات المتبادلة، والتأكد من أن لدينا بنية تحتية متنوعة ومرنة حقًا.

أما الجانب الآخر فهو أنه لا يمكنك أبدًا التنبؤ بدقة بما سيحدث. لذا، عليك أن تفترض أن الكوارث ستحدث. والأمر يتعلق أكثر بالتدرب على الخدمات واستعادتها عندما تحدث تلك الكوارث. وهذا يتطلب ممارسة، ليس فقط داخل مؤسستك، ولكنك تحتاج بالفعل إلى ممارسته مع عناصر أخرى من سلسلة التوريد. لكن دعونا نعود إليكِ يا فيونا.

(FIONA ALEXANDER) شكرًا يا بروس. والمتحدث الأخير لدينا، دان.
فيونا ألكسندر

(DAN YORK) أحييكم. شكرًا لكم جميعًا على تقديم هذه الجلسة النقاشية في فعالية ICANN. هذا وقت حاسم بالنسبة لنا للتفكير في هذا النوع من المرونة.
دان يورك

أريد أن أتطرق إلى موضوع مختلف قليلًا، وأتحدث عن شيء موجود في سيراليون الآن، وهو عبارة عن حاوية بطول 40 قدمًا تم تجديدها مثبتة على هيكل شاحنة. إنها تجوب البلاد، وتغير حياة النساء والفتيات. إنه جزء من مشروع يسمى صالون الشاحنات الرقمية، وهو يوفر التدريب والمعلومات للأشخاص، وكثير منهم يستخدمون الإنترنت لأول مرة.

فهو يوفر التدريب، ويوفر الإرشاد، ويوفر جوانب أخرى. وقد حقق نجاحًا باهرًا. تعلمت فاطمة، وهي امرأة تدير مشروعًا لتحويل الأحذية، كيفية الإعلان، وانتشر فيديو "قبل وبعد" الخاص بها على نطاق واسع، مما أدى إلى زيادة قاعدة عملائها ودخلها.

امرأة أخرى تدعى ماري، وهي خياطة، تعلمت كيفية تسويق تصاميمها، وهي الآن تعرض إبداعاتها بفخر في مقاطع الفيديو. وقد ساهم وجودها على الإنترنت في زيادة مبيعاتها من خلال مجموعة أعمالها على واتساب. وتحدثت امرأة أخرى عن كيفية زيادة إيراداتها بنسبة 95%.

هذه أنشطة تغير مجرى الحياة. وهناك ملايين القصص الأخرى المشابهة في كل مكان. وإذا نظرنا إلى سبب نجاحهم، فذلك لأنهم كانوا يمتلكون الإنترنت، بالطبع، ولكنهم كانوا يمتلكون أيضًا نظام اسم النطاق DNS لدوراتهم التدريبية، وقدراتهم، والخدمات التي ما

زالوا يستخدمونها بطريقة أو بأخرى. هذا هو الجزء الحاسم في سبب حاجتنا إلى الحديث عن المرونة هنا في ICANN.

تلعب مؤسسة ICANN دورًا حاسمًا في ضمان مرونة واستمرار تشغيل النظام البيئي المحيط بنظام اسم النطاق والمعرفات الأخرى. ومع ذلك، عندما ننظر إلى الأمور، نجد أن مؤشر مرونة الإنترنت الذي نحافظ عليه في حالة نبض مستمر. مجتمع الإنترنت. تُظهر المؤسسة أن مناطق مثل أفريقيا جنوب الصحراء الكبرى وأجزاء من منطقة المحيط الهادئ تحصل على حوالي 30 إلى 40 من أصل 100، مما يعني أنها تعمل بالفعل على بنية تحتية هشة في بعض الأحيان مع هامش ضئيل للفشل.

عندما يتعطل الإنترنت في أي اقتصاد، فإن ذلك لا يقتصر على تعطيل الخدمات فحسب. إنها تقطع سبل العيش عن أمثال فاطمة وماري. إنها تقطع الوصول إلى الخدمات الحكومية والرعاية الصحية عن الأشخاص الذين لا يملكون في بعض الأحيان أي بديل. ومع انتقالنا إلى المزيد والمزيد من الأنظمة إلى البنية التحتية العامة الرقمية، وإلى المزيد والمزيد من الخدمات بطرق مختلفة، فإننا نزيد من الاعتماد والحاجة إلى وجود إمكانية الوصول إلى الإنترنت هناك.

علينا أن ننظر إلى مرونة المؤسسات. علينا أن ننظر إلى المرونة التقنية. علينا أن ننظر إلى المرونة البشرية، أينما كانت. هناك أماكن هنا يمكننا أن نتعلم فيها. توجد أماكن في جميع أنحاء العالم أيضًا. يمكننا أيضًا أن نتعلم الكثير من الاقتصادات الناشئة. تحدث السيد سينغ للتو عن الانقطاعات الهائلة التي شهدناها في أماكن مختلفة حول العالم.

أود أن أشير إلى أنه قبل عامين، كنت أقوم بتوثيق حالات انقطاع الإنترنت، وشاهدنا ما كان انقطاعًا هائلًا للتيار الكهربائي في بورتوريكو. انقطع التيار الكهربائي عن حوالي 90% من البنية التحتية. وفكرت، حسنًا، سيتوقف الإنترنت، أليس كذلك؟ في الواقع، انخفض قليلًا، لكنه استمر. لذلك، تواصلت مع شخص ما من فرعنا في بورتوريكو هناك وسألته: لماذا؟ ماذا حدث؟ ما الذي أبقاه يعمل؟ وكان جوابه أن الناس هناك لا يعتمدون على شبكة الكهرباء. إنهم يفترضون أنها ستفشل. وهكذا، قاموا ببناء قدرة شخصية على الصمود باستخدام ألواح شمسية وبطاريات رخيصة للحفاظ على تشغيل أجهزة توجيه الواي فاي الخاصة بهم.

قامت شركات الاتصالات بتركيب مولداتها وأنظمتها الخاصة للعمل معها. هناك دروس في المرونة يمكننا تعلمها من كل مكان حول ذلك. ومن الأهمية بمكان أن نفعل ذلك. هناك الكثير مما نحتاج إلى القيام به والتفكير فيه، لأن هناك أيضًا 2.2 مليار شخص ما زالوا غير متصلين بالإنترنت. وكل انقطاع نشهده يؤدي أيضًا إلى تآكل الثقة في الإنترنت ويجعل الحاجة إلى الاتصال أكثر صعوبة في بعض الأحيان.

نحن لا نخسر وقت التشغيل فحسب. إننا نخسر النقاش حول جدوى الاستثمار في الإنترنت. لذلك، هناك الكثير مما نحتاج إلى القيام به والكثير مما يمكننا القيام به داخل مجتمع ICANN وداخل مجتمع الإنترنت الأوسع لضمان حصول أشخاص مثل ماري وفاطمة والناس في كل مكان على إنترنت موثوق به ومرن. أتطلع إلى بقية محادثاتنا هنا.

(FIONA ALEXANDER) فيونا ألكسندر: شكرًا لك يا دان. وشكرًا لجميع المتحدثين. سأعيد الآن الكلمة إلى رام ليقدم لنا أول موضوع من المواضيع الثلاثة التي سنتناولها اليوم.

(RAM MOHAN) رام موهان: شكرًا لك، فيونا. لدينا ثلاثة مواضيع رئيسية لخبرائنا اليوم. تزايد تعقيد النظام ونقص تمويل الرعاية الوقائية. التبعيات الدائرية ومخاطر سلسلة التوريد. وأخيرًا، دور مؤسسة ICANN في تعزيز مرونة الإنترنت. لنبدأ مناقشتنا بالنظر إلى الحجم الهائل للأنظمة التي ندير ها اليوم.

لم يعد الإنترنت مجرد مجموعة من أجهزة التوجيه والكابلات. إنها شبكة ضخمة من واجهات برمجة التطبيقات وخدمات الحوسبة السحابية وموردي الطرف الثالث. تحدث بول فيكسي عن ذلك للتو في بيانه الافتتاحي. نحتاج إلى التحدث عما يحدث عندما يتجاوز هذا التعقيد قدرتنا على إدارته. لذا، بالنسبة للجنة، السؤال الأول، يمكن للتطبيقات الحديثة أن تعتمد على 30 إلى 40 واجهة برمجة تطبيقات مختلفة وخدمات خارجية. متى يصبح التعقيد نفسه هو التهديد، ومن المسؤول عن إدارته؟ من يرغب في معالجة هذا السؤال؟

(SHRI M. A. K. P. SINGH) سأعالج ذلك.
شري ماكب سينغ

(RAM MOHAN) تفضل.
رام موهان

(SHRI M. A. K. P. SINGH) يا سيد رام، في الواقع، عندما نتحدث عن هذا العدد من واجهات برمجة التطبيقات المختلفة وخدمات الطرف الثالث التي نوفرها، والتي نرغب في إبقاء أنظمتنا قيد التشغيل، فإننا نخلق مشكلة الصندوق الأسود لأنه لا يوجد شخص واحد يفهم مخططات التبعية بأكملها، في الواقع.
شري ماكب سينغ

لذا، فإن جعل عملية استكشاف الأخطاء وإصلاحها مجرد تخمين، هو مجرد تخمين. وعلاوة على ذلك، عندما يكون لدينا الكثير من واجهات برمجة التطبيقات التي نقوم بدمجها في نظامنا لأغراض الكفاءة والمرونة، فهناك عوامل هجوم محتملة على سلسلة التوريد، في الواقع. لذا، نقوم بتوسيع نطاق ثقتنا لإدارة هذا الأمر، ولكننا لا نستطيع إدارته في بعض الأحيان.

ونحن نثق في بعض الأطراف مثل دان يورك الذي استشهد بمثال مستشعر CrowdStrike Falcon، حيث تعطلت أجهزة Microsoft Windows في يوليو/تموز 2024 عندما تم دفع التصحيح الذي لم يتم اختباره بالكامل تلقائيًا إلى نواة Windows، ولم يتمكن العديد من مشغلي الرحلات الجوية من تقديم الخدمات للركاب لإصدار بطاقات الصعود إلى الطائرة أو عرض حالة رحلاتهم.

لذا، يصبح هذا النوع من البيئة معقدًا، ونحتاج إلى تقليل الاعتماد على واجهات برمجة التطبيقات وخدمات الطرف الثالث، وإلا سيصبح الأمر غير مرئي.

(RAM MOHAN)
رام موهان

شكرًا. بول، اسمح لي أن أسألك، هل توافق أم لا توافق على ما قاله السيد سينغ للتو؟ وإذا كنت تتحدث، فنحن لا نسمعك. يمكننا سماعك الآن.

(PAUL VIXIE)
بول فيكسي

وأود أن أضيف أن التعقيد له الدور في الأنظمة الرقمية الذي تلعبه الحرارة في الأنظمة الفيزيائية. إنه منتج نفايات ولا يمكنك التخلص منه بسهولة. لذا، كلما توسعنا في هذا الأمر، خضعنا لحكم الآخرين، وسيحكم مصيرنا قانون الأعداد الكبيرة، بحيث يزداد عدد الافتراضات التي يضعها الآخرون حول ما ستفعله، والتي لا تعرفها أبدًا، والعكس صحيح، بلا حدود، ويكون لها التأثير الذي وصفه السيد سينغ.

(RAM MOHAN)
رام موهان

شكرًا. بروس، هل لديك رأي في هذا الأمر أيضًا؟ ليس في هذه المرحلة. حسنًا، عظيم.

حسنًا، دعني أطرح السؤال التالي. تمتلك الشركات العملاقة في مجال الحوسبة السحابية الموارد والانضباط التشغيلي اللازم لاختبار سيناريوهات الفشل بشكل روتيني وشامل إلى حد ما. ماذا يحدث يا داني للمنظومة ككل عندما لا يفعل ذلك المشغلون الأصغر الذين يعتمدون عليهم؟

(DANNY MCPHERSON)
داني ماكفرسون

أجل، لذا أعتقد أنك ترى أشياءً مثل تلك التي رأيتها مع CrowdStrike، أليس كذلك؟ حيث يقوم الأشخاص بنشر وكيل برمجي يمكنه تحديث المدخلات وتعديل النوى وإنشاء بيئة تجريبية أو بيئة اختبار قبل القيام بذلك. وترى انقطاعات كهذه.

مع ذلك، لست مقتنعًا بأن لدى شركات الحوسبة السحابية العملاقة سجلًا أفضل بكثير من معظم مشغلي الأنظمة الآخرين اليوم، بالنظر إلى كثرة حالات الانقطاع التي شهدناها مؤخرًا، لكن لديهم بالتأكيد الكثير من القدرات، والكثير من الحجم والتأثير والعواقب. وبالتالي، أصبح الأمر أكثر وضوحًا. لذا، لن أنتقدهم من هذا المنظور، ولكن في الوقت نفسه، يميلون إلى التحرك بسرعة ويكون لهم تأثيرات كبيرة حتى عندما يرتكبون أخطاء صغيرة.

لذا، أعتقد أنه من العدل ألا يتمتع الأشخاص ذوو الموارد المحدودة أو الأشخاص الذين لديهم قدرات أقل بنفس القدرة. أعتقد أن المسؤولية تقع على عاتق الجميع للتأكد من أننا نطور أفضل الممارسات الحالية، ونصمم قدرات مرنة وقوية حتى لا نصاب بفشل القلب عند حدوث الأخطاء، قدر الإمكان. إذن، تكون متقدمًا على الوقت.

(RAM MOHAN)
رام موهان

شكرًا يا داني. دان، لقد كنت تراقب هذا الأمر وتقوم بقياس ودراسة مرونة الإنترنت لفترة طويلة. أنت تدير مؤشرًا؛ لقد شاركت في إدارة مؤشر. إذن، من وجهة نظرك ومن منظورك الخاص، ما هي سيناريوهات الفشل التي تقلقك أكثر من غيرها اليوم؟

(DAN YORK)
دان يورك

حسنًا. لقد أخذت الأمر في اتجاه مختلف عن الاتجاه الذي كنت أقصده. أعتقد أن مرونة الإنترنت لا تتجاوز مرونة أضعف حلقاته. وأعتقد أن الحلقة الأضعف في العديد من المناطق هي مزود خدمة الإنترنت الصغير، ربما الوطني، أو نقطة تبادل الإنترنت IXP التي لا تملك ميزانية مخصصة للمرونة بطريقة أو بأخرى. أعتقد أن الشيء الذي يبقيني مستيقظًا هو قدرة المنظمات المحلية على التعافي والعمل معنا.

أعتقد أن التبعيات هي ما لا نفهمه جيدًا. وهذا يعود إلى الأشياء التي قلتها في البداية يا رام. علينا أن ننظر بشكل شامل للغاية إلى كيفية ترابط كل هذا. ما هي سلاسل التوريد؟ ما هي الصلاحيات؟ ما هي مسارات النقل؟ ما هي أنظمة الدفع؟ كيف يرتبط كل ذلك بطرق مختلفة؟

أعتقد أن أحد الجوانب الحاسمة في هذا الموضوع، والتعامل مع هذا التعقيد، هو النظر تحديدًا في كيفية تطوير الخبرات الفنية المحلية؟ كيف نقوم بإنشاء بنية تحتية محلية للربط الشبكي؟ كيف نُنشئ مجتمعات تقنية محلية؟ كيف نقوم ببناء القدرات لمساعدة الناس على فهم الإنترنت وبنائه في أماكن تواجدهم؟

لقد رأينا أن بناء القدرات لا يقل أهمية عن المعدات أو البروتوكولات أو أي شيء آخر. لقد رأينا مرارًا وتكرارًا أن المجتمعات المحلية المدربة تتعافى من انقطاعات التيار الكهربائي بشكل أسرع بكثير من تلك التي تعتمد على شخص بعيد جدًا أو ما شابه.

لذا، أعتقد أن هذا يبني على ما قاله داني للتو. هناك حاجة ماسة لتحديد أفضل الممارسات ومشاركتها. وهناك أيضًا حاجة للتأكد من وجود أشخاص في الميدان، قادرين على الذهاب وبناء وصيانة وإصلاح البنية التحتية للإنترنت بطريقة ما. وهذا ما يجعلها أكثر مرونة.

(RAM MOHAN)
رام موهان

شكرًا لك يا دان. كارلوس، هل لدينا نتائج من استطلاع الرأي الأول على Mentimeter؟ ما هو السبب الأكبر للاضطراب العالمي القادم الذي أثاره استطلاع Mentimeter؟ حسنًا، بينما ننتظر أن يثير كارلوس هذا الموضوع، اسمحوا لي أن أطرح سؤالًا آخر على هذه اللجنة.

نسمع باستمرار أن المرونة هي مشكلة وقائية استباقية، ولكن أيضًا أن الوقاية لا تجذب الأموال. إذن، يا بروس، من المسؤول في هذه المنظومة عن المرونة، ومن يتحكم في الميزانيات، وما الذي يتطلبه الأمر لتغيير حسابات تخصيص الميزانيات للوقاية بدلًا من تخصيصها لردود الفعل؟

(BRUCE TONKIN)
بروس تونكين

نعم، أعتقد أن جزءًا من ذلك هو القدرة على توضيح المخاطر بشكل صحيح لأولئك الذين يملكون الميزانيات بطريقة ما. أعني، هناك أموال متاحة. وكلما نظرت إلى أمور المرونة، فأنت بحاجة حقًا إلى توضيح المخاطر بشكل واضح وشرح ما يمكن أن يحدث بشكل خاطئ ولماذا، وكيف أن تطبيق أموال إضافية من شأنه أن يعالج تلك المخاطر بشكل كبير.

(RAM MOHAN)
رام موهان

شكرا لك يا بروس.

(SHRI M. A. K. P. SINGH)
شري ماكب سينغ

هل يمكنني أن أضيف شيئًا؟

(RAM MOHAN) تفضل.
رام موهان

(SHRI M. A. K. P. SINGH) في معظم الأحيان، عندما كنتُ مسؤولًا رئيسيًا عن أمن المعلومات، كما هو الحال عندما يتوجه مسؤولو أمن المعلومات إلى مجلس الإدارة لطلب تمويل لتدابير الأمن السيبراني أو لضمان مرونتهم، يطرح المجلس دائمًا العديد من الأسئلة، وتحتفظ الإدارة المالية بالتمويل، في الواقع، بالمقترحات.

شري ماكب سينغ

لذا، فقط عندما يدركون ذلك عند وقوع حادث ما. في إحدى الحوادث الأخيرة التي وقعت في هجوم جاكوار لاند روفر، تكبدت الشركة خسارة قدرها 1.9 مليار جنيه إسترليني. إنها خسارة فادحة. حتى الحكومة البريطانية اضطرت للتدخل.

في ذلك الوقت، أدركت تلك الشركة أنه كان ينبغي عليها إنفاق الكثير من المال على ذلك لضمان مرونة عملية التصنيع الخاصة بها. لذا قبل أن يكون رد الفعل هو الحل، يجب أن يكون المرء استباقيًا وأن يمول هذه الميزانية فعلًا لضمان آليات الوقاية للمرونة.

(RAM MOHAN) شكرًا يا سيد سينغ. كارلوس، أفترض أنك ستنشر النتائج عندما تكون مستعدًا لذلك. لذا، إذا قبلنا أن التعقيد يتجاوز ميزانياتنا المخصصة للوقاية، فعلينا أن ننظر إلى أين يكمن هذا التعقيد بالفعل. وتتزايد أهمية الأنظمة غير المرئية التي تقع خارج شبكاتنا الخاصة، والتي أصبحت على نحو متزايد أضعف الحلقات. إذن، فيونا، دعيني أترك لكِ المجال للنظر في موضوعنا الثاني، وهو التبعيات الدائرية ومخاطر سلسلة التوريد.
رام موهان

(FIONA ALEXANDER) شكرًا جزيلًا يا رام. إذن، كما ذكرت، فقد أوضحت هذه الجلسة الأولى بعض هذه التبعيات الدائرية التي لدينا. ونحن ننظر إلى بيئة يحتاج فيها الإنترنت إلى شبكة الكهرباء ليعمل، ولكن شبكة الكهرباء تحتاج بشكل متزايد إلى الإنترنت لكي يتعافى. والأمر لا يقتصر على
فيونا ألكسندر

البنية التحتية المادية فقط. وهو أيضًا الكود مفتوح المصدر المدفون في خمس طبقات عميقة داخل برنامجنا.

إذن، السؤال الأول للسيد سينغ. يُظهر لنا انقطاع التيار الكهربائي في شبه الجزيرة الأيبيرية عام 2025 أن انقطاع التيار الكهربائي يتحول إلى انقطاع الإنترنت الذي يتحول بدوره إلى انقطاع التيار الكهربائي. هل يعلم قطاع الطاقة أنه يعاني من مشكلة في الإنترنت؟ وهل يعلم مجتمع الإنترنت أنه يعاني من مشكلة في الطاقة؟ ما رأيك في ذلك؟

(SHRI M. A. K. P. SINGH)
شري ماكب سينغ

عندما نتحدث عن هذا الهجوم على البر الرئيسي لشبه الجزيرة الأيبيرية، فقد أثر في الواقع على ما بين 50 إلى 60 مليون شخص. وكل ذلك بسبب أمرين أو ثلاثة أمور مهمة يجب ملاحظتها هنا، وهي أن معظم الطاقة المتولدة كانت من مصادر الطاقة المتجددة، الطاقة الشمسية وطاقة الرياح. إنها متصلة بشكل ضعيف بالشبكات الرئيسية، وهذه العناصر لا تمتلك قصورًا ذاتيًا. ولهذا السبب، عندما ينقطع التيار الكهربائي، لا تستطيع الشبكة تحقيق الاستقرار.

لذا، عندما نتحدث عن امتلاك قدرة تركيبية كبيرة جدًا من الطاقة المتجددة، فإن هذه الإخفاقات ستحدث. وفي ذلك الوقت، نحتاج إلى أن تكون بنيتنا التحتية الرقمية أكثر أمانًا. كما هو الحال في هذه الحالة، توقف هذا النظام المستقل عن إعلان بادئات IP بمجرد حدوث انقطاع التيار الكهربائي فعليًا. لذا، في حالة البرتغال وإسبانيا، انخفضت حركة الإنترنت في البرتغال بنسبة 90% وكان الجفاف في إسبانيا أقل حدة، كل ذلك بسبب امتلاكهم المزيد من مصادر الطاقة الاحتياطية.

لذا، في حالة انقطاع التيار الكهربائي أيضًا، إذا كان لديك مصدر طاقة احتياطي أفضل، فستتمكن من الحفاظ على بنيتك التحتية الرقمية. وعندما تصبح البنية التحتية الرقمية جاهزة للعمل، ستتمكن من استعادة إمدادات الطاقة لديك بطريقة أسرع. هذا هو الدرس الأول والأهم الذي يمكن استخلاصه منه. وقد رأينا بالفعل أن العديد من الأجهزة الموجودة تتطلب الحد الأدنى من الطاقة أيضًا. كما هو الحال عند إجراء عمليات التبديل، يجب أن يكون مستوى البطارية 75% لتشغيل وإيقاف قواطع الدائرة الكهربائية في قطاعات الطاقة، والتي تعتبر مهمة لجلب واستعادة الإمداد. إذن، هذا ما تتطلبه البنية التحتية.

(FIONA ALEXANDER)
فيونا ألكسندر

شكرًا جزيلًا على هذه المداخلات. يقع مشغلو ccTLD عند مفترق طرق حرج بين سياسة ICANN والبنية التحتية الوطنية. ما مدى تعرض المشغلين المسجلين لمخاطر سلسلة التوريد التي لا يمكنهم حتى رؤيتها؟ وهذا السؤال موجه إلى بروس بصفته مشغل رمز بلد.

(BRUCE TONKIN)
بروس تونكين

أجل، شكرًا يا فيونا. أعتقد أن أحد أهم الأمور هناك هو أنك تحتاج بالفعل إلى أن تطلب من موردِيك أن يرسموا لك خريطة توضح كيفية تكوين خدمتهم. بمعنى آخر، تصميم الشبكة أو التصميم المادي والموردين الرئيسيين الذين يستخدمهم مزود الخدمة الخاص بك لتقديم الخدمة.

إحدى المشكلات، لقد تحدثنا قليلًا عن التعقيد سابقًا، ولكن ما لاحظته هو أنه في أي منظمة معينة، يوجد شخص أو شخصان يفهمان كل هذا التعقيد في أذهانهما. إذا فقدت أحد هؤلاء الأشخاص، أو لم يكونوا متاحين لأنهم خارج نطاق الاتصال لسبب ما، فأنت في ورطة لأن الكثير من ذلك غير مدوّن. وبالتالي، لا يوجد بديل إذا لم يكن ذلك الشخص الرئيسي موجودًا.

لذا فإن المفتاح بالنسبة لبنيتك التحتية الخاصة، وخاصة سلسلة التوريد الخاصة بك، هو أن تجعلهم يقدمون لك المعلومات على شكل رسم تخطيطي، إذا أردت، لنظامهم وموردِيهم، وأن تجعلهم يشرحون لك خطة إدارة المخاطر الخاصة بهم، وأن تجعلهم يقدمون لك نسخًا من عمليات التدقيق التي ربما قاموا بها من خلال خدمات خارجية، مثل تدقيق ISO 27001، وأن تجعلهم يعملون معك في تمارين الأمن السيبراني حتى تفهم بالفعل ما هو موجود في سلسلة التوريد الخاصة بهم.

(FIONA ALEXANDER)
فيونا ألكسندر

شكرا جزيلا لك، بروس. إذن، فإن الاستنتاج الرئيسي هنا هو أننا عرضة للخطر، وشبكاتنا عرضة للفشل المتتالي من خارج قطاعاتنا، حتى لو كان كل شيء مهيأ بشكل مثالي في شبكاتنا الخاصة. لكننا هنا اليوم في اجتماع ICANN. لذا، علينا أن نسأل أنفسنا، ما هي

المهمة المحددة لـ ICANN ومجتمع ICANN في كل هذا، وهو ما يقودنا إلى موضوعنا التالي. شكرًا.

(RAM MOHAN)
رام موهان

وقبل أن نفعل ذلك يا كارلوس، هل نذهب إلى استطلاع الرأي الثالث في Mentimeter؟ هل أنت مستعد لذلك؟ إذن، لدينا استطلاع رأي آخر. لذا، أيها الحضور، يرجى التقاط هواتفكم ومسح هذا الرمز. والسؤال الذي نطرحه عندما يظهر ذلك على الشاشة هو: إذا انقطعت شبكة الطاقة الرئيسية في منطقتك أو مزود الخدمة السحابية تمامًا لمدة 72 ساعة، فما مدى ثقتك في أن خدماتك الأساسية ستستمر؟

إذن هذا سؤال، سيظهر على الشاشة. لذا، وبينما نقوم بذلك، فهذا هو موضوع نقاشنا الأخير اليوم. لنعد الأمر إلى مؤسسة ICANN. لا يمكننا إصلاح شبكات الطاقة في العالم. لا يمكننا إصلاح كل مكتبة مفتوحة المصدر. لا يمكننا حل كل مشكلة جيوسياسية تحدث. لكننا ما زلنا جميعًا مسؤولين عن نظام المعرف الفريد للإنترنت.

إذن، أين تتقاطع مهمة مجتمع ICANN مع واقع الهشاشة البيئية التي تتجلى بوضوح في العالم من حولنا؟ إذن يا داني، ما الذي يتطلبه الأمر فعلًا لكي تتفاقم هشاشة الأنظمة مثل البنية التحية الأساسية للمفتاح العام أو الامتدادات الأمنية لنظام اسم النطاق إلى شيء كارثي بشكل كبير؟

(DANNY MCPHERSON)
داني ماكفرسون

هل قمت بإلغاء كتم الصوت؟ حسنًا، ها نحن ذا. لذا، أعتقد أن بروتوكول نظام اسم النطاق نفسه قوي بطبيعته. وتجعل ممارسات التنفيذ والتشغيل منه أكثر قوة. توجد طبقة تخزين مؤقت لاستيعاب حالات الفشل، وقد أثبتت الكيانات التي تشغل العناصر الأساسية لتلك البنية التحتية براعتها التشغيلية.

أعتقد أنه إذا نظرت إلى وقت التشغيل وسجلات تتبع نظام خادم الجذر أو بعض عمليات التسجيل هناك، فإنها تتجاوز بكثير أي عمليات سحابية أو أشياء أخرى. لذا، أعتقد أن لديهم سجلًا حافلًا بالإنجازات. ومع ذلك، فقد كانت هناك بالتأكيد حالات فشل متعلقة بـ DNSSEC، لكن معظمها يعود إلى الخبرة والنظافة التشغيلية الأساسية.

بالتأكيد هناك سيناريوهات يمكنك تخيلها حيث تؤدي أعطال RPKI إلى عدم استقرار التوجيه، مما يتسبب في تعطل DNS وكل ما يعتمد على التوجيه، مما يمنع إصلاح RPKI لأنه يعتمد على DNS للعمل، أليس كذلك؟ لذا، أعتقد أن هذا هو أسوأ سيناريو ممكن. لكن مع ذلك، أعتقد أن السبب الرئيسي الذي دفع معظم المشغلين اليوم إلى تطبيق المخازن المؤقتة أو ضوابط أخرى مثل تخفيض تفضيلات التوجيه بدلًا من سيناريوهات الفشل التام هو أن هذا يمثل في حد ذاته هجومًا لتخفيض مستوى الأمان الذي توفره لك هذه الضوابط.

لكن هذه الأمور توفر بعض المتانة وتراعي المقايضات التشغيلية الحكيمة. لكنني أعتقد أنه كما نرى، يعتمد RPKI على DNS ويعتمد DNS على التوجيه، والتبعيات الدائرية تشكل مشكلة عندما تحاول هندسة خطط الاسترداد أو مقاومة الأعطال، ولكن بالتأكيد المرونة في مواجهة الأعطال حتى تتمكن من التراجع والتعافي منها وتوفير مستوى معين من الخدمة والقدرة على العودة إلى وضع التشغيل الطبيعي. لذا، أعتقد أن هذا سؤال وجيه يا رام.

(RAM MOHAN)
رام موهان

شكرًا يا داني. إذن يا دان، غالبًا ما يكون المجتمع المدني والمستخدمون في الاقتصادات الناشئة هم الأكثر عرضة للخطر عندما تفشل الأنظمة. وأيضًا يا سيد سينغ، هذا شيء سأطرحه عليك بعد قليل، لكن دعني انتقل إلى دان أولًا. ما هي التكاليف البشرية التي لا نتحدث عنها بما فيه الكفاية؟

(DAN YORK)
دان يورك

سؤال رائع يا رام. وأعتقد أن التحدي يكمن في أننا لا نغير العالم، أعني أن التكاليف البشرية تكمن في أننا لا نغير العالم. نحن لا نصنع تأثير الأشياء. إذا نظرنا إلى المجتمع المدني، وإذا نظرنا إلى المنظمات في القطاع غير الربحي أولًا، فإن التحدي يكمن في أنها لا تمتلك في كثير من الأحيان موارد الشركات.

إن تمويلهم وجهودهم تركز على مهمتهم وبرنامجهم، وليس بالضرورة على تكنولوجيا المعلومات أو البنية التحتية لتكنولوجيا المعلومات، سواء كان ذلك إطعام الجياع أو تعليم المهارات الرقمية أو الدفاع عن حقوق الإنسان عبر الإنترنت، وسواء كانت مدرسة أو

كنيسة أو مكتبة أو أي شيء آخر، فإن التركيز ينصب على المهمة، وتغيير العالم له الأولوية.

عادة ما تكون البنية التحتية لتكنولوجيا المعلومات ذات أولوية أقل. غالبًا ما تعتمد تلك الأسئلة التي طرحتها للتو في Mentimeter على أنظمة خارجية. لا يمكنهم بالضرورة النهوض من جديد بطريقة أو بأخرى.

لذا، هنا تكمن أهمية المجتمعات التقنية المحلية، والمجموعات المحلية من هذا القبيل، في قدرتها على المساعدة في عملية التعافي وبناء تلك المرونة البشرية للتمكن من الذهاب والمساعدة في العمل على ذلك. أعتقد أنك تسأل في هذا القسم عما يمكن أن تفعله مؤسسة ICANN، وأعتقد أن مؤسسة ICANN ومجتمعها يمكن أن يلعبا دورًا حيويًا هنا.

إن ضمان وجود نظام DNS ومعرف مرن أمر بالغ الأهمية، ولدينا مجتمع كبير وعالمي تابع لـ ICANN يمكنه المساعدة. ذكر داني سابقًا موضوع أفضل الممارسات. أعتقد أن هناك إجراءً ملموسًا يمكن أن تتخذه مؤسسة ICANN. بالطبع، ينظر المرء إلى هذه التبعيات والأجزاء، ولكن ماذا لو تمكن مجتمع ICANN من تحديد نقاط الفشل المحتملة في الأجزاء المختلفة من منظومة المعرفات؟

تحديد أفضل الممارسات لكل قطاع، سواء كان ذلك خوادم الجذر، أو السجلات، أو أمناء السجلات، أو مزودي خدمة الإنترنت، أو مشغلي محلل النطاقات المتكرر، أو الشركات، أو المنظمات غير الربحية. ماذا لو استطعنا تطوير هذه الممارسات داخل مجتمع ICANN ثم الترويج لأفضل الممارسات من خلال مختلف الدوائر ومجموعات أصحاب المصلحة؟

يمكن لأعضاء شبكة مزودي خدمة الإنترنت التحدث إلى مزودي خدمة الإنترنت، ويمكن لدائرة الأعمال التحدث إلى الشركات، ويمكن لمجموعة أصحاب المصلحة غير التجاريين التواصل مع المنظمات غير الربحية، وهكذا دواليك. يمكنك أن تذهب وتأخذ أفضل الممارسات هذه وتنظر في كيفية قيام كل جزء من مجتمع ICANN ببناء المرونة لضمان استمرار عمليات ومرونة نظام اسم النطاق.

أعتقد أن هذا شيء ملموس للغاية يمكن أن تقوم به مؤسسة ICANN في هذا السياق لأن هذه التكاليف البشرية هي تكلفة عدم الوفاء بتلك المهام، وعدم تلبية ما يبحث عنه المجتمع المدني. وكما تحدثنا سابقًا أيضًا، فإن الاقتصادات الناشئة غالبًا ما تكون أكثر اعتمادًا على

بعض تلك الأنظمة الأكبر حجمًا. نحن بحاجة إلى بناء تلك الخبرة المحلية، وبناء تلك القدرات البشرية المحلية، وهكذا نجعل الأمور أكثر مرونة.

(RAM MOHAN)
رام موهان

شكرًا لك يا دان. سيد سينغ، هل ترغب في التحدث بإيجاز عن هذا السؤال المتعلق بالتكلفة البشرية للمرونة؟

(SHRI M. A. K. P. SINGH)
شري ماكب سينغ

انظر، سأعطيك مثالًا كلاسيكيًا، مثل عندما يتأثر مصدر الطاقة. كما ذكرت في جلسة الترحيب الصباحية، فإن نصف مراكز البيانات في الهند موجودة في مومباي. وكما تعلمون، في عام 2020، حدث انقطاع للتيار الكهربائي لمدة ست ساعات في مومباي. وأنت تعلم حجم فقدان البيانات الذي كان من الممكن أن يحدث لو استمر انقطاع التيار الكهربائي لفترة أطول.

وخاصة في مناطق النزاعات الحربية، كما هو الحال مؤخرًا في أجزاء مختلفة من العالم، حيث أن معظم مرافق البنية التحتية الرقمية غير متاحة بسبب الاضطرابات. كما سألتني فيونا عن شبه الجزيرة الأيبيرية، في الواقع، عندما حدث هذا الانقطاع، لم يتمكن الناس من شراء حتى خبزهم وزبدتهم، لأن كل شيء أصبح رقميًا.

لذا، بدون إنترنت، لا يمكن لأحد إجراء المعاملات. إذن، هذه هي التكاليف. وعلاوة على ذلك، فإن المساعدات الإنسانية التي نرغب في تقديمها، لا يمكننا تقديمها في ظل هذه الظروف. وفي الواقع، هناك جوانب أخرى لهذه المشكلات، مثل هذا، عندما تعمل أنظمتنا في وضع متدهور أثناء انقطاع التيار الكهربائي أو أي شيء آخر، فإن الهجمات الإلكترونية تكون أكثر نشاطًا، والمتسللون أكثر نشاطًا، كما هو الحال عندما أردنا مؤخرًا تقديم المساعدات الإنسانية إلى ميانمار، فقد تأثرت طائراتنا التي تحمل المساعدات الإنسانية بانتحال نظام تحديد المواقع العالمي.

يمكننا الهبوط بعد تشغيل الوضع اليدوي. لذا، تتأثر هذه المرافق، وفي كثير من الأحيان قد تتحول إلى كوارث إذا لم يكن لدينا بعض المرافق الاحتياطية.

(RAM MOHAN)
رام موهان

شكرًا جزيلًا. لدينا الآن الاستطلاع الرابع على Mentimeter. يظهر على الشاشة. وما نسأله هنا، بالنظر إلى المشهد الأوسع لمرونة الإنترنت، هو أين تكمن نقطة الضعف الأكثر أهمية لدى مجتمع ICANN الآن؟ إذن، هذا سؤال.

والآن دعونا ننتقل إلى المجتمع. يوجد ميكروفونان هنا في الممر الأوسط. لذا، من فضلكم، إذا كانت لديكم أي أسئلة، تفضلوا بالصعود إلى الميكروفون لطرحها علينا. أما بالنسبة للمشاركين عن بُعد، فيرجى استخدام ركن الأسئلة والأجوبة. لدينا وقت قصير فقط، لذا يرجى جعل أسئلتكم موجزة ومختصرة، لا تتجاوز 90 ثانية. هل هناك أي أسئلة من الجمهور؟ كاثي؟

(KATHY SCHNITT)
كاثي شنيت

نعم، مايكل باليج، يمكنك إلغاء كتم الصوت وطرح سؤالك.

(MICHAEL PLAGE)
مايكل باليج

مايكل باليج. هل يمكنكم سماعي؟

(RAM MOHAN)
رام موهان

نعم.

(MICHAEL PALAGE)
مايكل باليج

ممتاز. شكرًا لك يا رام. في الجلسة الافتتاحية اليوم، استمعنا إلى APNIC حول الأدوار الحاسمة لسجلات الإنترنت الإقليمية في منظومة الإنترنت. سؤالي هو، لماذا تم تجاهل حرف N الثاني في ICANN إلى حد كبير في نقاش اليوم؟ السؤال الثاني للمتابعة، على عكس الأسماء التي لدى ICANN اتفاقيات قانونية مع معظم نطاقات المستوى الأعلى

العامة، فإن لدى ICANN فقط مذكرة تفاهم مع منظمة مصادر الأرقام NRO، وهو كيان غير قانوني.

إذن، من وجهة نظر سلسلة التوريد، هل يمثل ذلك نقطة ضعف معينة؟ ثم السؤال الثالث، ما هي الاعتبارات المحتملة لمكافحة الاحتكار بالنسبة لـ ICANN ومشغلي معرفات الإنترنت الفريدة؟ هل يشكل ذلك تهديدًا أمنيًا أو تهديدًا للاستقرار؟ نرحب بأي متحدثين يرغبون في الإجابة على أي من هذه الأسئلة الثلاثة. شكرًا.

(RAM MOHAN)
رام موهان

شكرًا لك، مايك. داني، اسمح لي أن أنتقل إليك وأسألك ما إذا كنت ترغب في تغطية أحد هذه الأسئلة الثلاثة.

(DANNY MCPHERSON)
داني ماكفرسون

نعم، يسعدني ذلك. أعني، نحن نقضي الكثير من الوقت في العمل مع الأعضاء، من منظور تشغيلي في وظيفتي اليومية، الكثير من الوقت في العمل مع ثلاثة من سجلات الإنترنت الإقليمية التي نحن أعضاء فيها ونتابع الكثير من تطوراتها عن كثب. إن البنية التحية الأساسية للمفتاح العام RPKI، الذي له تأثيرات تشغيلية أكبر على البنية التحتية، وتأثيرات تشغيلية مباشرة أكبر على البنية التحتية التي نقوم بتشغيلها، قد أثار قلقنا.

ونريد التأكد من أن هذه البنية التحتية قوية وآمنة. والاستثمارات في ذلك مهمة. والأشخاص الذين يديرون هذه العمليات يلتزمون بمعايير محددة ويجسدون الأمن والبراعة التشغيلية التي نتوقعها من أي من موردي خدماتنا. لذا، فإننا نقضي الكثير من الوقت في ذلك. وأعتقد أن الأمر أصبح أكثر أهمية الآن مما كان عليه في أي وقت مضى، أليس كذلك؟ أعني، قبل خمس سنوات، لم أكن مضطرًا للقلق بشأن RPKI على الإطلاق.

والآن عليّ أن أقلق بشأن نطاق الهجوم التشغيلي الخاص بي والقدرات التي توفرها سجلات الإنترنت الإقليمية هذه، وأن أخطط لمواجهة حالات فشل ذلك. أعتقد أن سجلات الإنترنت الإقليمية قد قامت بعدد من الأشياء لتعزيز متانة البنية التحتية.

كان أحد تعليقاتي الافتتاحية يتعلق بالأنظمة ذات الارتباط الضعيف وبعض المخازن المؤقتة الموجودة لبعض هذه الضوابط في حالة حدوث أعطال. وعلى سبيل المثال، يفرض آرون

ذلك من خلال بعض الانقطاعات المخطط لها في بنيتهم التحتية. للأسف، أو لحسن الحظ، أعتقد أن مشغلي سجلات النطاقات الفاخرة لا يملكون ذلك، لكنني أعتقد أن سجلات النطاقات الإقليمية تعمل بالتأكيد على تحسين قدراتها في هذا المجال.

أعتقد أن حالة سلسلة التوريد للبرمجيات التي تُمكّن RPKI والاستثمار والتمويل الخاص بسجلات الإنترنت الإقليمية RIR أمر بالغ الأهمية لضمان استمرار البنية التحتية التشغيلية التي توفرها في تعزيز قدراتها والحفاظ على أمنها وقوتها. لذا، أعتقد أن هذا كل ما سأقوله بخصوص ذلك.

(RAM MOHAN) شكرًا يا داني. لنأخذ سؤالًا من هنا في الغرفة.
رام موهان

(ANAND RAJE) مرحبًا. أناند راجي من مؤسسة الإنترنت الهندية، وذلك لسجلاتنا. إذن، نحن محاطون بواجهات برمجة التطبيقات ونتحدث عن ذلك.
أناند راجي

(RAM MOHAN) بطيء. لا، تحدث في الميكروفون.
رام موهان

(ANAND RAJE) مرحبًا؟
أناند راجي

(RAM MOHAN) نعم.
رام موهان

(ANAND RAJE)
أناند راجي

أجل. وتعتمد خدمات النظام عبر هويات الإنترنت في الغالب على بنى الثقة المركزية. سؤالي للجنة هو: ما هو تأثير بنية الثقة المركزية على مرونة الإنترنت الإقليمية؟

(RAM MOHAN)
رام موهان

شكرًا. بول، هل تريد أن تعالج ذلك؟

(PAUL VIXIE)
بول فيكسي

سأفعل، ولكن هل يمكنك إعادة السؤال؟ أعد طرح السؤال.

(RAM MOHAN)
رام موهان

ما هو تأثير بنية الثقة المركزية على مرونة الإنترنت الإقليمية؟

(PAUL VIXIE)
بول فيكسي

في الوضع الطبيعي، هذا أمر مثير للقلق للغاية. بمعنى آخر، لقد شهدنا أوقاتًا لم تكن فيها مرونة الاتصال كافية بين بعض المناطق وبقية العالم. وكان هناك تبعية متبادلة بحيث لم تتمكن الأنظمة المحلية من العثور على أنظمة محلية أخرى أو لم تتمكن من تحديد ما إذا كانت ستثق في أنظمة محلية أخرى لأن أيًا منهما لم يتمكن من الوصول إلى نظام بعيد جدًا.

مرة أخرى، يحدث هذا بشكل افتراضي. إنه أمر يجب على كل مصمم أن يبحث عنه. ولهذا السبب، تستحق التصاميم، وليس فقط التطبيقات، أن تخضع لاختبارات فريق الاختبار الأحمر. وبعبارة أخرى، فإنها تستحق اختبارًا عدائيًا من قبل أشخاص يحاولون اكتشاف هذه العيوب قبل تشغيلها.

(RAM MOHAN)
رام موهان

شكرًا لك، بول. كاثي، هل لديكِ أي أسئلة أخرى من الإنترنت؟

(KATHY SCHNITT)
كاثي شنيت

لدينا سؤال عبر الإنترنت موجه إلى بروس. رفعت أستراليا مستوى الأمن السيبراني إلى مستوى حقيبة وزارية مع تعيين وزير متخصص. هل عزز هذا التغيير بشكل ملموس نهج الحكومة تجاه أمن نظام اسم النطاق والمرونة السيبرانية الأوسع نطاقًا، أم أن التحدي الحقيقي لا يزال يتمثل في التنفيذ عبر الوكالات والقطاعات المختلفة؟

(BRUCE TONKIN)
بروس تونكين

هذا سؤال صعب. أعتقد أن ما فعلته أستراليا من وجهة نظر الحكومة هو أنها أنشأت وزارة للشؤون الداخلية وحاولت تجميع الكثير من الوظائف الأمنية عبر مختلف الوكالات في تلك الوزارة. ومن خلال تلك الإدارة، قاموا بإنشاء تشريع يسمى قانون أمن البنية التحتية الحيوية.

وبالتالي، هذا هو الشيء الرئيسي الذي يؤثر علينا كمشغل سجل، وهو، إن صح التعبير، مجتمع من مشغلي البنية التحتية الحيوية. لكن نطاق صلاحيات وزير الأمن السيبراني أوسع من ذلك، إذ يشمل جميع قطاعات الصناعة، وليس جميعها يُعتبر من مزودي البنية التحتية الحيوية. وهذا ينطبق بشكل خاص على الشركات الصغيرة. وبالتالي، هناك أيضًا جهد موازٍ في كيفية رفع مستوى الوعي بالأمن السيبراني بين الشركات الصغيرة؟ وما هي الأمور العملية التي يمكنك القيام بها لمساعدة الشركات الصغيرة على تحسين أمان أنظمتها؟

لذا، أود أن أقول إن الوزير ربما يركز بشكل أكبر على الأمن السيبراني الأوسع نطاقًا للشركات الصغيرة، في حين أن تفاعلنا كمشغل سجل يكون مع مزودي البنية التحتية الحيوية الآخرين من خلال وزارة الشؤون الداخلية.

(RAM MOHAN)
رام موهان

شكرا لك يا بروس. لنستمع إلى سؤال من الحضور هنا.

(IDIL KULA)
إيديل كولا

مرحبًا. هذه إيديل كولا من تركيا، للعلم فقط. أنا زميلة ICANN. إذن، جميع أعضاء اللجنة يتحدثون عن المرونة والقوة والبنية التحتية التشغيلية المستمرة للإنترنت ككل. وكما ذكرتَ مجددًا، إنها الشبكة الكاملة التي لا تقتصر على البنية التحتية فحسب، بل تشمل أيضًا واجهات برمجة التطبيقات والخدمات السحابية وموردي الطرف الثالث.

إذن، الشيء الوحيد الذي لم أسمعه هو أنك تتحدث عن مخاطر سلسلة التوريد ومخاطر الطاقة. لكن لكي يستمر الإنترنت ويتمتع بالمرونة، نحتاج أولًا إلى المرونة البيئية والإيكولوجية، لأننا نعتمد على البيئات للحصول على الطاقة اللازمة للمرونة واستمرارية الإنترنت.

إذن، كيف تعتقد أن بإمكان مؤسسة ICANN تشجيع جميع أصحاب المصلحة من أجل تبني ممارسات أكثر استدامة ومسؤولية؟ لأننا جميعًا مجتمع واحد من جميع أنحاء العالم. إذا كان هناك جهة واحدة قادرة على فرض وتشجيع الناس على اتباع ممارسات أكثر استدامة ومسؤولية، فهي الجهة التي أشعر بها. ينبغي أن يكون هذا هو المكان.

لذا سؤالي هو: كيف يمكننا القيام بالتشجيع بشكل شامل؟ لأننا إذا انتظرنا الحكومات أو الجهات الفاعلة الإقليمية لفرض مسؤوليات المناخ، فسيكون الوقت قد فات بالتأكيد. وفي نهاية المطاف، إذا لم تتوفر لدينا كميات كافية من المياه لاستمرار سلاسل الإمداد، فلن يكون لدينا حاليًا أي استمرارية للإنترنت.

(RAM MOHAN)
رام موهان

شكرًا. لذا، اسمح لي أن أحيل هذا السؤال إليك يا دان. ما رأيك فيما يمكن أن تفعله مؤسسة ICANN للمساعدة في تعزيز المرونة البيئية؟

(DAN YORK)
دان يورك

كم من الوقت لدينا يا رام؟ أعتقد أن هناك سؤالًا أكبر، لم نتمكن من سماع السؤال الفعلي عبر الإنترنت يا رام. لذا، إذا أمكنك تكرار جزء منه.

(RAM MOHAN)
رام موهان

نعم، لقد لخصت الأمر لك. ما رأيك فيما يمكن أن تفعله مؤسسة ICANN للمساعدة في قضايا البيئة وتغير المناخ والمرونة البيئية والإيكولوجية؟ لذا دعوني فقط -- لأن الوقت ينفد. لذا، أنا فقط أقوم بتلخيص الأمر.

(DAN YORK)
دان يورك

حسنًا، أقدر ذلك. لذا، أعتقد أن هناك قدرًا كبيرًا من العمل يجري داخل منظومة الإنترنت الأوسع حول هذه الأنواع من قضايا المناخ. ينظر بعضهم إلى الحوسبة الخضراء، وكيفية تشغيل مراكز البيانات، وكيفية تشغيل الأنظمة على مستوى أفضل وأكثر ملاءمة للكربون، أي باستخدام طاقة أقل.

هناك سلسلة كاملة من الأمور هناك. ليس لدي توصيات محددة في الوقت الحالي، باستثناء القول بأنه عند النظر إلى سلسلة التوريد بأكملها، وعند النظر إلى جميع الأجزاء والأنظمة المختلفة، فإن لكل منها مكانًا يمكن من خلاله دراسة تأثيراتها على أزمة المناخ؟ ما مقدار الطاقة التي يستخدمونها؟ كيف يمكنهم تقليل بصمتهم في مجال الطاقة؟ كيف يمكنهم جعل الأنظمة تعمل بطريقة أكثر ملاءمة للكربون؟

يمكن القيام بكل هذه الأنواع المختلفة من الأشياء على كل مستوى من مستويات التسلسل الهرمي، سواء كان ذلك من السجلات إلى أمناء السجلات إلى مزودي خدمة الإنترنت الفرديين إلى الأشخاص الذين يستخدمون شبكات توصيل المحتوى أو تشغيل خوادمهم الموثوقة الخاصة. هناك أماكن في ذلك المكان يمكن فيها أخذ كل ذلك في الاعتبار. قد يكون هذا مسار عمل آخر يمكن أن تتولاه مؤسسة ICANN للنظر في كيفية جعل هذه الأنظمة ضمن نظام DNS ونظام المعرفات أكثر ملاءمة للمناخ.

(RAM MOHAN) رام موهان: شكرًا لك يا دان. كارلوس، اسمح لي أن آتي إليك وأسألك عما إذا كان بإمكانك عرض ومشاركة نتائج استطلاعات Mentimeter مع جمهورنا. إذن، إليك ما قلته بشأن ما تعتقد أنه سيكون السبب الأكبر للاضطراب العالمي القادم. حسنًا، لننتقل إلى الرد التالي، السؤال التالي.

(SHRI M. A. K. P. SINGH) شري ماكب سينغ: أهلًا سيدي. اسمي هو--

(RAM MOHAN) رام موهان: انتظر قليلًا. أنا الآن بصدد مراجعة إجابات أسئلة Mentimeter. وهل هناك أي ردود أخرى على الاستطلاع؟ يرجى الانتقال إلى التالي. لذا، وبفارق كبير، فإن ما يقال هو أن التنسيق بين القطاعات، والتواصل مع قطاعات الطاقة والاتصالات وغيرها، يمثل نقطة الضعف الأكثر أهمية لدى مجتمع ICANN. هذا ما يُظهره هذا الاستطلاع.

وهل هذا كل شيء يا كارلوس؟ حسنًا، عظيم. شكرًا جزيلًا لكم. دعوني أنتقل الآن إلى أعضاء فريقنا. ودعني أبدأ بك يا بروس، أولًا. وهذا سؤال سأطرحه على جميع أعضاء اللجنة. لو كان لديك القليل من الوقت للتحدث مباشرة إلى قيادة ICANN بعد هذه الجلسة العامة، فماذا ستقول لهم أن الأمر يجب أن يحدث أولًا؟

(BRUCE TONKIN) بروس تونكين: أعتقد أننا بحاجة إلى بذل جهد لرسم خريطة لسلسلة التوريد الخاصة بالسجلات وموفري نظام اسم النطاق والبحث عن التبعيات الرئيسية، ثم تشغيل بعض السيناريوهات إذا كانت بعض هذه التبعيات الرئيسية بها مشاكل. لذا، سأعطي مثالًا واحدًا: يستخدم الكثير منا برنامج BIND. ماذا سيحدث إذا كانت هناك مشكلة في BIND وقمت بتشغيل بعض السيناريوهات؟

(RAM MOHAN)
رام موهان

شكرًا. بول، ما الذي ستقوله لقيادة ICANN الذي يجب أن يحدث أولًا بعد هذه الجلسة؟

(PAUL VIXIE)
بول فيكسي

لم نتحدث كثيرًا في هذه الجلسة عن الضغوط التنظيمية، لكنني أعلم أن شيئًا مثل COICA يمكن أن يظهر فجأة لحماية الملكية الفكرية. إذا لم نذهب إلى كاليفورنيا ونقول، حسنًا، لقد طلبت للتو التحقق من العمر، بما في ذلك على المصادر المفتوحة، بما في ذلك الأنظمة غير المتعاقد عليها، فهذا لا يمكن أن ينجح. ما هي الأمور الأخرى التي تهمك حتى نتمكن من معرفة المزيد عنها قبل أن تقرر إقرارها كقانون؟

أعتقد أننا بحاجة إلى تواصل أوسع مع العالم، وخاصة الديمقراطيات، لمعرفة ما يرغبون في الحصول عليه من الإنترنت حتى نتمكن من بدء عملية بنائه لهم أو إخبارهم لماذا هو غير واقعي.

(RAM MOHAN)
رام موهان

سيد سينغ، ما الذي تود أن تطلبه؟

(SHRI M. A. K. P. SINGH)
شري ماكب سينغ

كما أظهرت نتائج Mentimeter، أود أن أقول إن الأعطال في نظام الطاقة قد تتسلسل عبر البنية التحتية الحيوية التابعة لها. لذا، قد يؤثر ذلك على الأمة أيضًا. نحن بحاجة إلى فهم كيف تتضافر جهود كيانات مثل المرافق الكهربائية ومراكز الاتصالات والعديد من مزودي الخدمات لدعم الوظائف الحيوية للحفاظ على البنية التحتية الرقمية قيد التشغيل.

(RAM MOHAN)
رام موهان

شكرًا. دان، ماذا ستطلب؟

(DAN YORK)
دان يورك

أود أن أقول ثلاثة أشياء. تحتاج مؤسسة ICANN إلى النظر في كيفية بناء تفكيرها التنظيمي حول المرونة ووضع ذلك في إطار التفكير الاستراتيجي أو كعنصر أساسي. يجب أن ينظر في المرونة التقنية. ما قاله بروس للتو والسيد سينغ حول رسم خرائط التبعيات الخفية لنظام اسم النطاق ونظام المعرفات، والنظر في أفضل الممارسات التي ذكرتها سابقًا والمرونة البشرية.

إذن، يتعلق الأمر بالجوانب التنظيمية والتقنية والبشرية المتعلقة بالمرونة، والنظر في كيفية القيام بذلك والاستفادة من المجتمع العالمي الذي لدينا. وأعتقد أن هناك العديد من المنظمات التي تعمل في هذا المجال والتي يمكن لـ ICANN أن تتعاون معها بطريقة أو بأخرى. لكن إذا حدث ذلك، فسنصل إلى مرحلة يمكننا فيها ضمان حصول الناس في كل مكان على إنترنت موثوق به ومرن.

(RAM MOHAN)
رام موهان

شكرًا. داني؟

(DANNY MCPHERSON)
داني ماكفرسون

أعتقد أن العديد من العناصر التي تحدثنا عنها متضمنة بالفعل في خطة ICANN الاستراتيجية هنا. أعتقد أنه من الواضح أن ICANN وهذا المجتمع من حيث الأنظمة التقنية والنطاق التقني قد قاموا بعمل مثالي في تشغيل البنية التحتية بطريقة آمنة ومستقرة، كما تعلمون، طوال الفترة التي قمنا بها. أعتقد أن هناك فرصة أوسع للتركيز على الآثار الخارجية للأشياء التي تؤثر على النظام. لست متأكدًا. أرى، كما تعلمون، في الاستطلاع هنا، نسبة 38% من التنسيق بين القطاعات.

أعتقد أن أحد الأمور التي يتم تجاهلها في بعض ذلك هو أن الكثير من الكيانات المسؤولة التي تعتبر من أصحاب المصلحة في مجتمع ICANN هذا تقضي وقتًا طويلًا بشكل مفرط في التركيز على التعافي من الكوارث، والاتصالات في حالات الطوارئ، ومرونة الأعمال، والعمل مع الشركاء، كما تعلمون، وسيناريوهات "ماذا لو" وتشغيل أنظمة مرنة.

لذا، لا أعرف ما إذا كان على ICANN القيام بذلك بشكل مباشر، ولكن بالتأكيد تعزيز ذلك وعناصر سلسلة التوريد الخاصة به وما إلى ذلك. لكنني أعتقد أنه من الناحية الاستراتيجية، فإن الشيء الذي لست متأكدًا من رؤيته هو التنبؤ بالاتجاهات والتهديدات، والنظرة الاستراتيجية لهذه الاتجاهات. ما هي التحولات الجيوسياسية والتقنيات الناشئة، والاضطرابات الاقتصادية التي قد تزعزع استقرار مؤسسة ICANN في هذا المجتمع؟

أعتقد أن فهم تلك القوى الخارجية ثم معرفة ما يقع ضمن نطاق اختصاص ICANN الأساسي ومجتمع ICANN هو أمر قابل للتنفيذ داخل مجتمع ICANN هنا.

(RAM MOHAN)
رام موهان

شكرًا يا داني. اسمحوا لي أن أسألكم جميعًا هنا في الجمهور، هنا في هذه القاعة، ارفعوا أيديكم، بعد الساعة الماضية، هل تشعرون أن مؤسسة ICANN بحاجة إلى جعل مرونة الإنترنت أولوية استراتيجية؟ حسنًا. حسنًا، جميل. فيونا، سأعود إليكِ لإبداء أي تعليقات أخيرة.

(FIONA ALEXANDER)
فيونا ألكسندر

أوه، أعتقد أنني سأتخلى عن تلك الأمور نظرًا لأننا تجاوزنا الوقت المحدد قليلًا، ولكن أشكر الجميع على عروضهم الرائعة، وآمل أن تكون الجلسة مفيدة للحاضرين عبر الإنترنت وفي القاعة، سواء عبر الإنترنت أو في القاعة، للتأكيد على أهمية أن يكون لكل فرد دور في مرونة الإنترنت.

(RAM MOHAN)
رام موهان

شكرًا جزيلًا. شكرًا لجميع أعضاء اللجنة، وقد انتهى الاجتماع.

(KATHY SCHNITT)
كاثي شنيت

يمكن إيقاف التسجيل الآن.

[انتهاء التدوين]