AR

(GULTEN TEPE)
غولتن تيبي:

مرحبًا بكم في جلسة اجتماع اللجنة الاستشارية الحكومية (GAC) مع اللجنة الاستشارية للأمن والاستقرار (SSAC) المنعقدة يوم الثلاثاء الموافق 28 أكتوبر/تشرين الأول، في تمام الساعة 15:00 بالتوقيت العالمي المنسق (UTC).

يُرجى العلم بأن هذه الجلسة يجري تسجيلها، وتحكُمُها معايير السلوك المتوقعة في ICANN، ومدونة قواعد السلوك الخاصة بمشاركي مجتمع ICANN، بالإضافة إلى سياسة مجتمع ICANN لمناهضة التحرش. خلال هذه الجلسة، لن تُقرأ الأسئلة أو التعليقات إلا إذا قُدمت بالصورة المناسبة في مربع الدردشة بتطبيق Zoom.

وستشمل الترجمة الفورية لهذه الجلسة اللغات الست للأمم المتحدة، إضافة إلى البرتغالية.

إذا كنت ترغب في التحدث أثناء هذه الجلسة، فيُرجى رفع يدك داخل غرفة Zoom، وذكر اسمك بغرض إثبات الحضور والتدوين في محضر الجلسة واللغة التي ستتحدث بها إذا كانت غير اللغة الإنجليزية. ونرجو التحدث بوتيرة مناسبة لضمان دقة الترجمة الفورية.

والآن، سوف أحيل الكلمة إلى نيكولاس كاباليرو، رئيس اللجنة الاستشارية الحكومية. شكرًا لكم.

(NICOLAS CABALLERO)
نيكولاس كاباليرو:

شكرًا جزيلاً لك، غولتن. أهلاً بكم جميعًا من جديد. آمل فعلاً أن تكونوا قد استمتعتم بتناول قهوة أيرلندية رائعة. يسعدني أن أقدّم صديقي العزيز وفريقه، رام موهان من اللجنة الاستشارية للأمن والاستقرار (SSAC)، ومعنا أيضًا سوزان ومارتن وتارا. أهلاً ومرحبًا بكم. سنخوض جلسة شيّقة للغاية – على الأقل من وجهة نظري – وهي مقسّمة إلى أربعة أجزاء.

الجزء الأول، والأهم في رأيي، يتناول أهمية FOSS (وهو اختصار يشير إلى البرامج الحرة مفتوحة المصدر) في مجال نظام أسماء النطاقات (DNS). ويمكنني إضافة أنها

ملاحظة: ما يلي هو ما تم الحصول عليه من تدوين ما ورد في الملف الصوتي وتحويله إلى 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. تُنشر هذه الملفات لتكون بمثابة مصادر مساعدة للملفات الصوتية الأصلية، ولكن ينبغي ألا تُعامل كما لو كانت سجلات رسمية.

مهمة في مجالات أخرى أيضًا، لكن هذا نقاش مختلف تمامًا. وبعدها ننتقل إلى مسألة تأثير تضارب السلاسل وتشابهها على الأمن والاستقرار، وهو موضوع لا يمكن تجاهله في هذه المرحلة. وأخيرًا، سنتناول مسألة إمكانيات التعاون بين اللجنة الاستشارية للأمن والاستقرار واللجنة الاستشارية الحكومية. ثمّ نفتح المجال لجلسة الأسئلة والأجوبة.

مرحبًا بكم مجددًا، وأُحيل الكلمة الآن إلى صديقي العزيز رام موهان. الكلمة لك.

(RAM MOHAN) رام موهان: شكرًا لك يا نيكو. يسعدني أن أكون هنا مجددًا معكم في دبلن، وكذلك بينكم في اللجنة الاستشارية الحكومية. نشعر فعلاً بالتقدير وكان شرفًا كبيرًا لنا أنكم ، وعلى مدار اجتماعات عدّة، واصلتم دعوتنا ومنحنا وقتًا ضمن جدول أعمالكم المزدحم. ومن جانبنا، فإننا لا نقدّر هذا الوقت فحسب، بل نستعد له بشكلٍ مكثّف، لأننا نحرص على أن تكون المعلومات التي نقدّمها، وطريقة تواصلنا وتفاعلنا معكم، على المستوى المناسب وقابلة للتطبيق، بحيث تحملون منها ما يفيدكم عمليًا. وهذا هو الأساس الذي ننطلق منه في عملنا.

ومن دون إطالة، أود تخصيص الجزء الأول من وقتنا للحديث عن أهمية البرامج الحرة مفتوحة المصدر في مجال نظام أسماء النطاقات. ولتقديم هذا الموضوع ومشاركة تفاصيله معكم، أُحيل الميكروفون إلى زميلي مارتن أرتسن، الذي كان أحد المشاركين في رئاسة مجموعة العمل المعنية بهذا الموضوع. تفضل يا مارتن.

(MAARTEN AERTSEN) مارتن أيرتسن: شكرًا لك يا رام، وشكرًا لك يا نيكو. اليوم سأتحدث إليكم عن البرامج. وعادةً ما تصدر اللجنة الاستشارية للأمن والاستقرار وثائق ذات طابع تقني إلى حدٍ كبير، لكن هذا التقرير ليس من هذا النوع ولا تنتمي إلى تلك الفئة، كما أن مجتمع ICANN ليس جمهورَه الأساسي. فهذه الوثيقة موجَّهة إلى صنّاع السياسات والجهات التنظيمية حول العالم. لذلك أعتقد أنني أتحدث إلى الجهة المناسبة. وإن لم تكونوا أنتم المعنيين، فأنا متأكد أن لديكم زملاء رائعين يعملون في مجال الأمن السيبراني.

دعونا نتحدث عن البرامج. إذا أردنا تلخيص تقريرنا في جملة واحدة، فسنقول إن نظام أسماء النطاقات قائم على البرامج الحرة مفتوحة المصدر. وهذا ليس نوعًا من الدعوة أو

الترويج، وليس تصريحًا بأن البرامج الحرة مفتوحة المصدر أفضل. إنه مجرّد بيان لحقيقة الطريقة التي بُني بها نظام أسماء النطاقات فعليًا. الشريحة التالية رجاءً

يشير الاختصار (FOSS) إلى البرامج الحرة مفتوحة المصدر. وكلمة حرة هنا تعني الحرية — مثل حرية التعبير — وليس مجانية السعر، أي أنها ليست مثل كوب غينيس المجاني الذي ستحصلون عليه بعد هذه الجلسة. تُعرَّف البرامج الحرة مفتوحة المصدر من خلال أربع حريات أساسية. الاستخدام — يمكنك استخدام البرنامج لأي غرض. الدراسة — يمكنك دراسة كيفية عمل البرنامج، بما في ذلك رمز المصدر الخاص به. المشاركة — يمكنك مشاركة البرنامج وإعادة توزيعه. التعديل — يمكنك تعديل البرنامج ليلبّي احتياجاتك وإصدار التحسينات.

هذه الحريات المضمنة في ترخيص البرنامج تخلق منظومة مختلفة جذريًا لتطوير البرامج وتوزيعها وصيانتها مقارنةً بالنموذج مسجل الملكية. وبينما توجد اختلافات فلسفية بين البرامج الحرة والبرامج مفتوحة المصدر، يستخدم هذا التقرير مصطلح البرامج الحرة مفتوحة المصدر ليشمل كلا المفهومين اللذين يتمحوران حول الحريات الأربع. الشريحة التالية رجاءً

يتميّز نموذج البرامج الحرة مفتوحة المصدر بنمط مخاطر مختلف عن البرامج مسجلة الملكية. فبما أن معظم البرامج الحرة مفتوحة المصدر يتم تطويرها وصيانتها بواسطة متطوّعين، فإن الدافعية تلعب دورًا كبيرًا. وعندما يعمل الناس على البرامج بشكلٍ تطوعي، فإنهم قد يشعرون بالإرهاق أو الاحتراق الوظيفي، مما يؤدي إلى توقّف المشاريع أو هجرها.

هناك أيضًا مخاطر أخرى في البرامج الحرة مفتوحة المصدر، مثل غياب الضمانات أو الدعم المضمون بشكلٍ افتراضي؛ لذلك يحتاج المشغّلون إلى تحمّل مسؤولية الاحتفاظ بخبرة التطوير داخل مؤسساتهم، أو ممارسة الحريات الأربع وإصلاح البرامج عند حدوث مشكلات، أو بدلاً من ذلك شراء عقود دعم.

وحين لا يتولى المتطوعون صيانة البرامج مفتوحة المصدر، بل تقوم بذلك جهات مهنية متخصصة، تظهر مشكلة الركوب المجاني، نظرًا لأن البرامج متاحة مجانًا للجميع. وقد تنشأ حالة ينفصل فيها التمويل تمامًا عن الاستخدام، بحيث يكون المشرف على الصيانة تابعًا لمبادرة صغيرة أو منظمة محدودة الموارد تتولى دفع رواتب القائمين على الصيانة.

وتكون هذه الجهات عرضة لصدمات تمويلية ناجمة عن أعباء تنظيمية جديدة. على سبيل المثال، عندما يتعرض نموذج التمويل الحالي للتهديد.

لذلك فهذه المخاطر حقيقية وملازمة لنموذج البرامج الحرة مفتوحة المصدر. كما أن أي تنظيم لا يأخذ هذه المقايضات بعين الاعتبار قد يجعل المخاطر أسوأ، وليس أفضل. الشريحة التالية رجاءً

لكن هناك أيضًا نقاط قوة. وهنا ننتقل للحديث عن نظام أسماء النطاقات تحديدًا بعكس الشريحة السابقة التي تناولت البرامج الحرة مفتوحة المصدر بشكلٍ عام. فعند النظر إلى هذا النظام، نلاحظ وجود قوة واضحة في الشفافية والتعاون الأمني. فالمجتمعان الأكاديمي والتشغيلي يحافظان منذ عقود على ثقافة متينة وفعّالة في فحص برامج نظام أسماء النطاقات الحرة ومفتوحة المصدر علنًا. ويمكن العثور على أبحاث تعود إلى التسعينيات تناقش عيوب البرامج أو طرق تحسينها. وهذه العيوب يجري مناقشتها بصراحة ومعالجتها.

وقد أعرب المشغّلون الذين شملهم الاستطلاع الذي أجريناه ضمن هذا البحث—وقد حصلنا على مساهمات من أكثر من 100 مشغّل— عن تقديرهم لقدرتهم على تشخيص الثغرات ونقاط الضعف والتحقّق منها وتصحيحها لأن سلسلة التوريد مفتوحة. فهم لا يعتمدون على سرعة استجابة المورّد، بل يمكنهم التحرّك بشكل استباقي.

وفي نظام أسماء النطاقات تحديدًا، فإن عددًا من مشاريع النظام الشائعة لا تُدار من قبل متطوّعين، بل من قبل مؤسسات مستقرة وطويلة العمر. وقد حافظت هذه المؤسسات على تطوير وتنفيذ البرامج لأكثر من 20 عامًا، مما يمنحها سجلاً ثريًا وموثوقًا يعتمد عليه المشغّلون.

ومن نقاط القوة الأخرى للبرامج الحرة مفتوحة المصدر في نظام أسماء النطاقات وجود مرونة تشغيلية عبر التنويع. فوجود عدة تطبيقات مختلفة من البرامج الحرة مفتوحة المصدر يُمكّن المشغّلين من تشغيل برامج متعددة، مما يقلل من نقطة الضعف المنفردة. كما أنه يخفض الحواجز أمام المؤسسات لتشغيل بنيتها التحتية الخاصة، مما يحد من مخاطر التركّز وكذلك، وهو موضوع يحظى باهتمام متزايد مؤخرًا، الاعتماد على جهات أجنبية. دعونا ننتقل إلى الشريحة التالية.

والآن لنتحدث عن الأمن. تركّز اللجنة الاستشارية للأمن والاستقرار بطبيعتها على الأمن، ومن المهم للغاية فهم العوامل الحقيقية التي تحدد مستوى الأمن. وما لا يحدد مستوى الأمن هو ما إذا كان رمز المصدر مفتوحًا أو مغلقًا. وما إذا كان المطوّرون متطوعين أو موظفين بأجر. وما إذا كان المشروع قادمًا من شركة تجارية أو منظمة غير ربحية.

بينما ما يحدّد فعليًا مستوى الأمن هو المراجعة الصارمة للرمز، والاختبارات الشاملة، ووجود آلية واضحة ومجرّبة للتعامل مع الثغرات، إضافة إلى صيانة نشطة وطويلة المدى مدعومة بموارد مستدامة.

وكما يرد في التقرير "إن أمن أي مشروع برمجي يعتمد على جودة عمليات التطوير والصيانة، وليس على مدى إتاحة رمز المصدر الخاص به".

كثيرًا ما نسمع السؤال التالي: هل البرامج الحرة مفتوحة المصدر أكثر أو أقل أمانًا من البرامج مسجلة الملكية؟ والإجابة: لا هذا ولا ذاك. فالأمن تحدّده جودة عملية التطوير، وليس نموذج الترخيص.

أما التحدّي على مستوى السياسات فيكمن في أن البرامج الحرة مفتوحة تحمل نمطًا مختلفًا من المخاطر. فلا يمكن ببساطة نسخ ولصق الأنظمة التنظيمية المستخدمة في عالم البرامج مسجلة الملكية وتوقع أن تعمل بالطريقة نفسها في بيئة تعتمد على البرامج الحرة مفتوحة المصدر.

لقد طرحتُ بعض الادعاءات القوية في البداية. ودعونا الآن نلقي نظرة على بعض البيانات. الشريحة التالية رجاءً بدءًا من مستوى نظام خادم الجذر، قمنا باستطلاع مشغّلي خوادم الجذر الاثني عشر، وحاولنا تحديد البرامج التي يستخدمونها. نلاحظ هيمنة واضحة لالبرامج الحرة مفتوحة المصدر. فهناك 9 على الأقل من أصل 12 مشغّلاً لخوادم الجذر يعتمدون بالكامل على البرامج الحرة مفتوحة المصدر. وحتى المشغّلين الذين يستخدمون برامج مسجلة الملكية للقيام بهذا الدور يقومون أيضًا بتشغيل البرامج الحرة مفتوحة المصدر بجانبها لأغراض التنويع والنسخ الاحتياطي. الخلاصة الأساسية هنا أن نسبة الاعتماد ليست صغيرة. فالبرامج الحرة مفتوحة المصدر تشكّل الغالبية الساحقة في نظام خوادم الجذر. الشريحة التالية رجاءً

علاوة على ذلك، قمنا بدراسة مشغّلي نطاقات المستوى الأعلى، وهم الجهات التي تقدم خدمات نظام أسماء النطاقات الموثوقة. وكانت النتيجة الأساسية أنه عند النظر إلى المشغّلين الذين يديرون أكبر عدد من نطاقات المستوى الأعلى، نجد أن 9 من أصل 10 منهم يستخدمون البرامج الحرة مفتوحة المصدر في البنية التحتية لنظام أسماء النطاقات.

والأمر الذي قد يكون أكثر أهمية لهذا الجمهور هو كيفية تطبيق ذلك في حيّز نطاقات المستوى الأعلى على صعيد البلدان. فعند النظر فقط إلى البلدان، نجد أن 20 من أصل 25 مشغّلاً يستخدمون البرامج الحرة مفتوحة المصدر. وبشكلٍ جماعي، يقوم مشغّلو نطاقات المستوى الأعلى لرمز البلد (ccTLD) بإدارة 234 نطاقًا فريدًا من نطاقات ccTLDs باستخدام هذا النموذج، وهذا فقط بناءً على المستوى الذي درسنا فيه البيانات. وبالتالي فالرقم الواقعي أكبر من ذلك.

وهذه ليست نطاقات مستوى أعلى صغيرة أو تجريبية؛ بل هي مزوّدو خدمات كبار مسؤولون عن ملايين النطاقات. على سبيل المثال: تستخدم نومينت في المملكة المتحدة البرامج الحرة مفتوحة المصدر، وكذلك يستخدمها مركز معلومات شبكة الإنترنت في الصين في الصين، وذلك على سبيل المثال لا الحصر. الشريحة التالية رجاءً

والآن لننظر إلى أنظمة السجل، وهي قواعد البيانات التي تخزن النطاقات داخل نطاق معين من نطاقات المستوى الأعلى. وهنا نرى نموذجين: نظام مبني بالكامل على البرامج الحرة مفتوحة المصدر. وهذا النموذج موجود، ورغم أنه ليس الأكثر انتشارًا، إلا أنه يثبت إمكانية العمل بهذا النموذج، وهو أمر مهم.

النموذج الأكثر شيوعًا هو أن يكون النظام مسجل الملكية. لكن حتى هنا نجد أن هذه الأنظمة مسجلة الملكية ليست مبنية من الصفر. بل عبارة عن تكاملات مسجلة الملكية مبنية فوق برامج حرة مفتوحة المصدر. ومن بين عشرة منصات رئيسية شملناها بالدراسة، وجدنا أن جميعها يعتمد على مكونات من البرامج الحرة مفتوحة المصدر. حتى عندما تكون منطقية الأعمال التجارية على المستوى الأعلى مسجلة الملكية، فإن الأساس يبقى مبنيًا على البرامج الحرة مفتوحة المصدر. الشريحة التالية رجاءً

يُعدّ نظام المحلّلات الأصعب من ناحية القياس، لكننا نجد مرة أخرى وجودًا قويًا ومكثفًا للبرامج الحرة مفتوحة المصدر. فهناك ثمانين في المائة من المستخدمين حول العالم يعتمدون على مُحلّل محلي، وفي هذا المجال تسود البرامج الحرة مفتوحة المصدر بشكلٍ

واضح. وحتى عند النظر إلى الحلول التجارية—وهي كثيرة—ففي معظم الحالات، إذا دقّقنا فيما يتم بيعه، سنجد أنه البرامج الحرة مفتوحة المصدر. وينطبق الأمر نفسه على المحلّلات العامة، فعدد منها يعتمد على البرامج الحرة مفتوحة المصدر أيضًا.

أجرينا كذلك دراسة حالة صغيرة في التقرير حول شركة "كلاودفلير"، التي تمتلك نواةً مسجلة الملكية محاطة ببرامج حرة مفتوحة المصدر. كما أن أربعة على الأقل من أكبر مزودي الخدمات السحابية يستخدمون البرامج الحرة مفتوحة المصدر لحلول نظام أسماء النطاقات لديهم. أما الآخرون، فيستخدمون مكتبات البرامج الحرة مفتوحة المصدر كمكوّنات داخل محلّلات مسجلة الملكية. الشريحة التالية رجاءً

واقتباسًا من التقرير "في أكثر الأجزاء حرجًا من بنية نظام أسماء النطاقات، تُعدّ البرامج الحرة مفتوحة المصدر هي الأساس الذي يُبنى عليه، بينما البرامج مسجلة الملكية هي الاستثناء". وهذا ليس مبالغة، ولا من باب المناصرة أو التحيّز؛ بل هو نتيجة صارمة توصلنا إليها من خلال البحث. فأنظمة التسمية الأساسية للإنترنت تعمل في الأساس على برامج تُطوَّر بشكلٍ تعاوني وتُوزَّع بشكلٍ حر. الشريحة التالية رجاءً

أما النهج التنظيمي التقليدي لسلسلة التوريد، فيتطلب وضع معايير أمنية—وربما يجري فرضها على مشغّلي البُنى التحتية الحيوية. ثمّ تتم محاسبة هؤلاء المشغّلين عند حدوث إخفاق، فيلجؤون بدورهم إلى موردهم ويضعون الشروط عليهم عبر العقود، وتُطبّق القواعد عبر آليات الشراء والوصول إلى السوق.

لكن لماذا يفشل هذا النهج في حالة البرامج الحرة مفتوحة المصدر؟ يرجع هذا لأن برامج البرامج الحرة مفتوحة المصدر غالبًا ما تكون متاحة للتنزيل مجانًا تمامًا، وقد لا توجد علاقة مع مورّد بالمفهوم التقليدي. فلا يوجد عقد بين المشغّل والمورّد—وفي كثير من الأحيان، لا يوجد "مورّد" أصلاً، بل هناك متطوّع.

إن فرض أعباء امتثال على المشغّلين بهدف التأثير على سلسلة التوريد قد يؤدي إلى زعزعة استقرار المؤسسات الصغيرة التي تتولى صيانة هذه البرامج تحديدًا. وإذا كان القائمون على الصيانة متطوّعين، فقد يفقدون الاهتمام أو الحافز، ما يؤدي إلى تخلّيهم عن المشاريع تجنّبًا للمخاطر القانونية، أو الانتقال إلى تراخيص مسجلة الملكية، أو حتى تجنّب

العمل ضمن ولايات قضائية معينة. والنتيجة هي أن البرامج التي يعتمد عليها الجميع تصبح أقل توفرًا وأقل أمانًا. الشريحة التالية رجاءً

لقد ضمّنا في التقرير دراسات حالة لأن ولايات كبرى مثل الولايات المتحدة والمملكة المتحدة والاتحاد الأوروبي بدأت في وضع سياسات تراعي خصوصية البرامج الحرة مفتوحة المصدر. ولن أخوض في تفاصيل هذه السياسات الآن إلا إذا كان هناك اهتمام، لكن ما يهم هو أنها ممكنة التطبيق. الشريحة التالية رجاءً

وإليكم خمسة إرشادات قابلة للتنفيذ توصّلنا إليها. فاللجنة الاستشارية للأمن والاستقرار لا تتخذ موقفًا بشأن ما إذا كان ينبغي لكم تنظيم هذا المجال أم لا. وليس من دورها إبداء رأي حول ذلك. ولكن إذا كانت هناك تنظيمات تُدرس في نطاقكم القضائي، فالرجاء أخذ الدور الحيوي للبرامج الحرة ومفتوحة المصدر في الحسبان. وأقِروا بأن البنية التحتية العالمية تعتمد عليها اعتمادًا كبيرًا، وأن هذا الاعتماد قوة يجب الحفاظ عليها.

وعليكم كذلك التواصل مع مجتمع البرامج مفتوحة المصدر. واحرصوا على إشراك القائمين على الصيانة والمؤسسات والمشغّلين في عملية وضع السياسات، وتجنّبوا العواقب غير المقصودة.

ويمكنكم الاستفادة من الدراسات المعاصرة التي جمعناها وتعلّموا من النماذج الجديدة التي بدأت بالظهور.

وقوموا أيضًا بتحفيز الاستدامة، وتشجيع — على سبيل المثال — المساهمات في البرامج الحرة مفتوحة المصدر باعتبارها استثمارًا في البنية التحتية العامة.

إضافة لذلك، تعاملوا مع المخاطر النظامية التي تُوجد عبر كامل منظومة البرامج، وليس في البرامج الحرة مفتوحة المصدر فقط، بشكلٍ جماعي. وادفعوا نحو تمويل حلول شاملة على مستوى المنظومة بغرض معالجة الاعتمادات المشتركة، بدلاً من تحميل العبء على القائمين على الصيانة فردًا فردًا.

أعتقد أننا وصلنا الآن إلى نهاية هذا العرض. وأتطلع الآن لسماع أسئلتكم.

(MARCO HOGEWONING) ماركو هوغوونينغ: شكرًا لك يا مارتن على هذا العرض الواضح والموجز. وكما نقلتُ رسالة رام في وقت سابق، أوصي الجميع بمتابعة الرابط وقراءة التقرير الفعلي.

ومن ناحية الوقت، لدينا مجال لطرح بعض الأسئلة. وأول سؤال في قائمة الانتظار لدي يأتي في الواقع من الشخص الجالس بجانبي.

(NICOLAS CABALLERO) نيكولاس كاباليرو: عذرًا، معي ممثل المفوضية الأوروبية.

(MARCO HOGEWONING) ماركو هوغوونينغ: حسنًا، سنستمع إلى ممثل المفوضية الأوروبية أولاً. شكرًا لكم.

(GEMMA CAROLILLO) جيما كارولليلو: شكرًا جزيلاً للرئيس ونائب الرئيس، ولكن يسعدني أن أعطي الكلمة لـ[غير مسموع] إذا كنت تفضل البدء أولاً. جيما كارولليلو، ممثل المفوضية الأوروبية. أظن أنّنا ضمن الجهات التي تخاطبونها، خصوصًا أن ثلاثة من أصل أربع دراسات حالة تنطبق علينا.

فهذا موضوع بالغ الأهمية بالنسبة لنا، وأودّ التأكيد أننا — بصفتنا جهة تنظيمية — قد تعلّمنا أيضًا من هذه العملية فيما يتعلق بكيفية إدماج الخصائص المختلفة للبرامج مفتوحة المصدر في التنظيم الرقمي. ويمكنني القول إن هذه كانت عملية صعبة ولكنها مفيدة للغاية، وأعتقد أننا نتعلم منها بشكلٍ جماعي ونحقق نتائج جيدة في الوقت الحالي.

وسؤالي يتعلق بأمن سلسلة التوريد، إذ يظل هذا الموضوع من المشكلات القائمة. حتى لو حاولنا الالتفاف حولها، تظل تمثل مشكلة مستمرة. فهل لديكم رأي بشأن مبادرات مثل "قائمة مكوّنات البرامج" وكيف يمكن أن تساعد فعليًا في معالجة مسألة أمن سلسلة التوريد؟ شكرًا لكم.

(MAARTEN AERTSEN)
مارتن أيرتسن:

شكرًا لك يا جيما. تسألين عمّا إذا كانت اللجنة الاستشارية للأمن والاستقرار لديها رأي بشأن "قائمة مكوّنات البرامج". وللأسف، أتحدث هنا باسم اللجنة، ولم نتناول هذا الإجراء تحديدًا. ويسعدني أن أقدّم لكِ رأيي الشخصي، وهذا تنويه مسبق بذلك.

نعم، الأمن يشكّل مشكلة في مجال البرامج — سواءً كانت برامج مسجلة الملكية أو برامج حرة مفتوحة المصدر. وأعتقد أن موضع فائدة "قائمة مكوّنات البرامج" يكمن في الحالات التي تشتري فيها الجهات أو المؤسسات برامج مسجلة الملكية يكون معظمها في الواقع مبنيًا على برامج حرة مفتوحة المصدر. ففي هذه الحالات، قد يكون أحد المكوّنات معرّضًا لثغرة، وتصبح هذه الثغرة مشتركة لدى الجميع، بل لدى جميع المنتجات الموجودة في السوق. وإذا لم يَعلَم المورّد — أو حتى المشتري — ما الذي يوجد داخل المنتج، فكيف يمكن البدء في معالجة المشكلة؟ ومن هذه الزاوية، فإن هذا النهج يعدّ أداة مثيرة للاهتمام. ومع ذلك، فما زلنا في مرحلة مبكرة.

وأقدّر كثيرًا تعليقك حول التعلّم الجماعي؛ ومن منطلق حديثي الشخصي، أجد أنه من المثير للاهتمام متابعة عملية وضع السياسات في الاتحاد الأوروبي، وسعيد بأن لدينا دراسة حالة تمكنّا من إدراجها في هذا التقرير.

(MARCO HOGEWONING)
ماركو هوغوونينغ:

شكرًا لك ممثل المفوضية الأوروبية على السؤال. شكرًا لك مارتن. لدي الآن ممثل بنغلاديش على قائمة المتحدثين، ثم رئيس مجلس الإدارة الجالس بجانبي. بعد ذلك سأغلق قائمة الطلبات مراعاةً للوقت، وننتقل إلى البند التالي. والآن، أحيل الكلمة إلى ممثل بنغلاديش، تفضّل رجاءً.

دكتور (SHAMSUZZOHA)
شمس الضحى:

شكرًا لكم. معكم شمس الضحى من بنغلادش. أعتقد أن هذا عرض ممتاز وشامل للغاية. وبشكلٍ خاص، باعتباري من بنغلاديش ومسؤولاً عن العمل مع عدد من الهيئات لوضع معايير الأمن في البلاد، فإن بعض ما ينتجونه يُعدّ من العناصر [يتعذر تمييز الصوت].

أنا مهتمّ من جانبين تحديدًا: أولاً، نحن نعمل أيضًا مع جهات مختلفة في بنغلاديش لوضع معاييرها الأمنية وكذلك [يتعذر تمييز الصوت]، وهذا يشمل كذلك نشر البرامج في سياق معيّن وضمن [يتعذر تمييز الصوت].

إضافة إلى ذلك، نحن مسؤولون عن الجلوس والتعاون مع البُنى التحتية الحيوية الوطنية، خصوصًا فيما يتعلق بوضع حلول CM وSWOT (القوة والضعف والفرص والتهديدات) لإدارة العمليات الأمنية.

وهنا تظهر لنا إشكالية عندما نحاول [يتعذر تمييز الصوت]—حتى داخل نظام المشتريات الحكومية—الترويج لاستخدام البرامج الحرة مفتوحة المصدر. لكن أحد الاعتراضات التي نواجهها يتعلّق بالقدرات الفنية المتاحة داخليًا في [يتعذر تمييز الصوت]، خصوصًا ضمن [يتعذر تمييز الصوت]، وكذلك الحاجة إلى متطلبات سريعة وفعالة.

ففي حال عدم وجود قدرة داخلية كافية، تظهر مخاطر كبيرة—خصوصًا عند التعامل مع البنى التحتية الوطنية الحسّاسة والحيوية، وكذلك إلى حدٍ ما فيما يتعلق بتكلفة التشغيل.

لذا قد يكون سؤالي—أو طلبي للحصول على رأيكم—هو: كيف يمكن التعامل مع هذه التحديات، خصوصًا عندما نتعامل مع بنى تحتية حساسة وحيوية؟ شكرًا لكم.

(MAARTEN AERTSEN)
مارتن أيرتسن:

شكرًا لكم. ومن هذه الزاوية، أعتقد أن الفجوة بين البرامج مسجلة الملكية والبرامج الحرة مفتوحة المصدر أقل مما قد يتصوّره البعض. فعند تشغيل بنية تحتية حيوية، تكون مسؤولية المشغّل هي الحفاظ على التشغيل السلس والمستقر. وإذا قررتم استخدام البرامج الحرة مفتوحة المصدر—وكما ذكرنا، هذا هو الخيار الأكثر شيوعًا—فإن أمامكم خيارين: امتلاك الخبرة داخل المؤسسة، وهذا يُعد تكلفة، إذ تحتاجون إلى وجود خبراء. أو الاستعانة بخبرات خارجية، وفي العديد من الحالات—عند النظر إلى أكثر البرامج شيوعًا—تكون المنظمات الداعمة لها مموّلة من عقود الدعم الفني.

أما لو كانت البيئة مختلفة ولم يكن هناك سوى البرامج مسجلة الملكية، فستقومون حينها بدفع تكاليف التراخيص، وفي الغالب تحصلون على الدعم الفني مقابل ذلك. ومن هذه

الناحية، أرى أنه لا يوجد اختلاف كبير، مع الأخذ في الاعتبار نقاط القوة التي ذكرناها في العرض — مثل عدم الارتباط القسري بمورّد واحد، وغيرها.

لكن نعم، البنية التحتية الحيوية لها خصوصيتها، فهي تحتاج إلى متطلبات جاهزية وتشغيل عالية، وتحتاج إلى خبرة فنية حقيقية لضمان ذلك. وكل مشغّل يمكنه اتخاذ قراراته بناءً على مدى الموارد والدعم الذي توفّره له حكومته لاتخاذ هذه الخيارات.

(MARCO HOGEWONING) ماركو هوغوونينغ: شكرًا لكما. شكرًا لكما. سنختتم الجلسة الآن، وسأمنح الكلمة لنيكو، بوصفه أحد أكبر الداعمين للبرامج الحرة مفتوحة المصدر.

(NICOLAS CABALLERO) نيكولاس كاباليرو: شكرًا لكم. سأكون مختصرًا في حديثي للغاية. وشكرًا لك يا مارتن على هذا العرض الرائع. هل يمكنك من فضلك أن تعلّق بشكل مختصر جدًا على كيفية مساهمة البرامج مفتوحة المصدر في تجنّب حالات الارتباط القسري بمورّد واحد بالنسبة للحكومات—وخاصة في الدول النامية—ليس فقط من ناحية التكلفة، بل أيضًا من ناحية ما يمكنني وصفه بتكاليف الأمن الداخلي؟

(MAARTEN AERTSEN) مارتن أيرتسن: الارتباط القسري بمورّد واحد هو الحالة التي تستثمر فيها في منتج معيّن ثم تعجز عن الانتقال منه لأن حجم الاستثمار أصبح كبيرًا جدًا أو لأن تكلفة التحويل مرتفعة.

أما ميزة البرامج الحرة مفتوحة المصدر في هذا السياق—بما في ذلك سياق الأمن السيبراني—فهي أنك لست مُلزَمًا بالاستمرار مع الجهة الأصلية التي قامت بصيانة البرامج. ففي كثير من الأحيان، توجد جهات أو منظمات أخرى قادرة على دعمك في عمليات التشغيل، بما في ذلك تطبيق التصحيحات.

صحيح أنك ستظل بحاجة إلى المطوّر الأصلي لتطوير التحديثات الأساسية، ولكن بخلاف البرامج مسجلة الملكية، لا توجد جهة واحدة فقط مجبرة على التعامل معها. ويمكن أن أتصوّر—وربما هذا رأيي الشخصي—أن بلدًا بميزانية محدودة قد يرى في هذا الأمر

فرصة لتعزيز الابتكار وبناء خبرة محلية بدلاً من دفع الأموال لجهات خارجية. لكن بالطبع، هذا خيار يعود لهم.

وأعتقد أن هذا هو أبرز ما يمكن قوله حول الارتباط القسري بمورد واحد. ومرة أخرى، هذا رأيي الشخصي نظرًا لأننا لا نتناول هذا الموضوع بشكلٍ موسّع في التقرير.

(MARCO HOGEWONING)
ماركو هوغوونينغ: شكرًا لك يا نيكو على السؤال، ولَك يا مارتن على إجابتك المميزة. وبناءً على الوقت المتاح لنا، دعونا ننتقل إلى الموضوع التالي، والذي دعوتُ فيه اللجنة الاستشارية للأمن والاستقرار أيضًا للمساهمة قليلاً في مسألة بناء القدرات. وللتذكير، أعلم أن هناك العديد من أعضاء اللجنة الاستشارية الحكومية الجدد أو الأحدث وجودًا في القاعة، وربما يكون هذا الموضوع جديدًا نسبيًا عليهم. لكنه موضوع مهم، ويزداد أهميةً كلما اقتربنا من الجولة القادمة. وبما أن سوزان موجودة معنا على الطاولة، أعتقد أنه يمكنني منحك الكلمة للحديث عن هذه النقطة. شكرًا لكم.

(SUZANNE WOOLF)
سوزان وولف: حسنًا شكرًا لك ماركو. وأتوجه بالشكر كذلك إلى مارتن. عمل مميز كالعادة، ومن الصعب مجاراتكما. وكما قال ماركو، سأبدأ بالحديث عن تضارب الأسماء في إطار مشروع تحليل تضارب الأسماء (NCAP)، وذلك نظرًا لأنني شاركت في رئاسة المشروع، وبرغم أن اللجنة الاستشارية للأمن والاستقرار هي الذي اقترحته في الأصل، لكنه نُفِّذ من خلال مجموعة نقاش من مختلف أطياف المجتمع.

وكما قال ماركو، ليس هناك كثيرون منكم ممن بقوا في المجتمع لفترة كافية ليتذكروا ذلك، لكن هذه ليست قضية جديدة. فقد واجهنا تحديات تضارب الأسماء للمرة الأولى في الجولة السابقة من نطاقات gTLD الجديدة. لكن كان علينا إعادة النظر فيها لأن عددًا من الأمور تغيّر، سواءً على مستوى التقنية أو التوقعات داخل بيئة الشبكة التي نعمل ضمنها. الشريحة التالية من فضلك. عذرًا، ارجع للخلف شريحة واحدة.

إذًا، ما هو تضارب الأسماء؟ يتبيّن أنه من الصعب للغاية وضع تعريف دقيق له، لكنه في الوقت نفسه من تلك الأشياء التي يمكن معرفتها عند رؤيتها. إحدى طرق تبسيط الفكرة هي

تشبيه أسماء النطاقات بعناوين المنازل. فإذا كان هناك منزلان يحملان العنوان نفسه، يصبح من الصعب تحديد أيهما يجب أن يستقبل البريد أو الطرود. وتوجد أيضًا مخاطر أمنية إذا وصل البريد إلى العنوان الخاطئ — فقط تخيّلوا الآثار المتعلقة بالخصوصية وحدها.

في نظام أسماء النطاقات، يحدث تضارب الأسماء عندما يُستخدَم نطاق ما في فضاء أسماء النظام العام — أي الإنترنت المفتوح كما نعرفه — ويُستخدم في الوقت ذاته في نطاق مختلف، مثل شبكة خاصة يديرها مزوّد خدمة الشبكة الافتراضية الخاصة، حيث تكون أسماء مختلفة صالحة وذلك أمر طبيعي، ولكن عندما يحمل الاسم ذاته معاني مختلفة، يمكن تفسير ما تبحث عنه بطريقة خاطئة. ويصبح الأمر مربكًا بسرعة كبيرة. الشريحة التالية من فضلك.

سنمر سريعًا على الشرائح القادمة لأننا نتجنب التفاصيل التقنية الدقيقة ونحاول الحفاظ على المستوى العام، لكن العرض الكامل سيكون متاحًا، ونحن دائمًا سعداء بمناقشة الجوانب التقنية بتفصيل أكبر عند الحاجة.

ما الذي لا يُعَدّ تضاربًا في الأسماء؟ بعض هذه المصطلحات سيكون مألوفًا لكم إذا كنتم تتابعون دليل مقدم الطلب أو أي عمل يُجرى حول نطاقات gTLD الجديدة. فتضارب الأسماء ليس — على سبيل المثال — مماثلاً لتشابه السلاسل أو السلاسل المتشابهة بصورة مربكة.

بل هو مشكلة تقنية تتسبب في وقوع مشكلات تتعلق بالأمن والاستقرار، وتنشأ عن تفويض نفس نطاق المستوى الأعلى المستخدم مسبقًا في سياق خاص. على سبيل المثال: example.corp في شبكتك الخاصة — إذا كان سيحمل المعنى نفسه كاسم في الإنترنت العام ولكنه يشير إلى شيء مختلف، فإنك تدخل في منطقة خطرة. تكمن الخطورة في أن الاستعلامات الخاصة بالأسماء في السياق الخاص قد تتسرّب إلى نظام أسماء النطاقات العام، وهو ما يسبب تضاربًا تقنيًا وإخفاقات أمنية.

يمثل تشابه السلاسل أيضًا تحديًا في مشروع نطاقات gTLD الجديدة وفي دليل مقدم الطلب، لكنه يرتبط أكثر بإدراك المستخدم. أي أنها مشكلة بشرية، وليست تقنية، وتؤدي إلى الارتباك بسبب نطاقات عليا عامة مختلفة لكن تبدو أو تُنطق بشكل متشابه للمستخدم. فإذا كان لديك كلمة "example" بحرف "l" صغير، ونفس الكلمة بحرف "I" كبير، يمكن أن

يختلط الأمر على المستخدم، مما يؤدي إلى مخاطر التصيّد والاحتيال والغش وفقدان ثقة المستخدم، إضافة إلى تأثير مباشر على المستخدمين.

الخلاصة هي أن هناك العديد من الطرق التي يمكن أن تنشأ بها مشكلات التضارب، لكن العنصر المهم هو أنه عندما يواجه الحاسوب غموضًا، يمكن أن تكون النتائج مربكة وخطيرة. الشريحة التالية. شكرًا جزيلاً.

الخلاصة على المستوى العام — بعيدًا عن التفاصيل التقنية — هي أن فهم تضارب الأسماء يُعد أمرًا مهمًا بالنسبة لأمن الإنترنت ويقع مباشرة ضمن مسؤولية ICANN في الحفاظ على أمن واستقرار جذر نظام أسماء النطاقات. وهناك مخاطر لعواقب غير مقصودة عندما تستخدم الشركات أسماءً كنطاقات مستوى أعلى داخلية قد تتسرّب إلى الإنترنت العالمي.

فإدخال مزيد من نطاقات gTLD الجديدة يزيد احتمالية ظهور هذه التحديات، لأن هناك مزيدًا من الأسماء التي قد تكون مستخدمة بالفعل في سياق خاص ولكن يجري أيضًا تفويضها في فضاء أسماء الإنترنت العام.

ويبقى قياس تضارب الأسماء مهمة صعبة—وسنخوض قليلاً في الأسباب—وذلك بسبب تطور التكنولوجيا وبنية الشبكات مع مرور الوقت، خصوصًا منذ الجولة السابقة من نطاقات gTLD الجديدة. فقد ظهرت تحسينات كبيرة في الخصوصية داخل نظام أسماء النطاقات، تجعل من الأصعب معرفة ما يحدث أو تتبُّع الاستعلامات، وهذا بالطبع جزء مقصود من هذه التحسينات. كما ظهرت أنظمة تسمية بديلة زادت من تعقيد مشهد النظام، وبالتالي أصبحت القياسات بشكلٍ عام أكثر صعوبة. الشريحة التالية.

لم أكن أمزح عندما قلت إن هذه القضية قديمة. شريحة واحدة إلى الأمام. الشريحة التالية. نعم، هنا. شكرًا لكم.

في عام 2012، أدّت جولة gTLD الجديدة إلى تسريع نمو ملف منطقة الجذر، مما أثار أسئلة حول ما قد يحدث عند إضافة سلاسل جديدة قد تكون مستخدمة بالفعل ضمن سياقات محدودة وغير معلنة في الجذر العام.

وفي عام 2013، تناولت اللجنة الاستشارية للأمن والاستقرار الموضوع وأصدرت استشارة رسمية حذّرت فيها من أن مشكلات كبيرة تتعلق بالأمن والاسقرار قد تنشأ نتيجة تضارب الأسماء.

والسلاسل الأكثر إشكالية، بعضكم ربما سمع بهذه الأمثلة الشهيرة، هيhome و.corp و.mail، وكانت هذه السلاسل مستخدمة على نطاق واسع للغاية في بيئات خاصة، لدرجة ظهور كمٍّ هائل من البيانات التي تُظهر مخاطر واضحة تجعل من الصعب جدًا—أو من غير الآمن—تفويضها في الجذر العام، أي نظام أسماء النطاقات العام.

وفي عام 2017، طلب مجلس إدارة ICANN من اللجنة الاستشارية للأمن والاستقرار إجراء دراسات شاملة تُمكّن من تنفيذ جميع عمليات تفويض نطاقات gTLD المستقبلية بطريقة آمنة ومستقرة وقابلة للتنبؤ.

ومن هذا التكليف ظهرت مشاريع تحليل تضارب الأسماء—وكان في الواقع مشروعين منفصلين—إلى جانب أسئلة متابعة من مجلس الإدارة.

وفي المرحلة الأخيرة، نُشرت الدراسة 2 لمشاريع تحليل تضارب الأسماء في أوائل عام 2024، وذلك لضمان أن النتائج والتوصيات التي توصلنا إليها يمكن أن تُستخدم في الجولة القادمة من نطاقات gTLD الجديدة.

كان إشراك فريق من مختلف مكوّنات مجتمع ICANN، وليس فقط من أعضاء اللجنة الاستشارية للأمن والاستقرار، تجربة جديدة بالنسبة لنا، وأعتقد أنها كانت خطوة ناجحة للغاية. فقد سمحت لنا بأن نبني على الأعمال السابقة والبحوث الأحدث بشكلٍ أكثر شمولاً. الشريحة التالية.

كان الهدف الأساسي لمشاريع تحليل تضارب الأسماء هو تحليل الوضع الحالي المتعلق باكتشاف حالات تضارب الأسماء والتعامل معها والتوصية بتحديث منهجية معالجة تضارب الأسماء استعدادًا للجولة القادمة من نطاقات gTLD الجديدة. وتم تقديم ذلك من خلال إطار جديد لتقييم المخاطر، لا يهدف فقط إلى تحديد وجود حالات تضارب بين الأسماء، بل أيضًا إلى تقدير حجم الضرر المحتمل وفهم طبيعة المخاطر وتحديد أنواع التخفيف الممكنة أو الوقاية التي يمكن تطبيقها.

نودّ أن نشير إلى أن عملية التقييم أصبحت أكثر صعوبة لأسباب متعددة — وقد ذكرنا بعضها بالفعل. وتَبيَّن أن أحد أكبر الأسباب هو أن قدرًا كبيرًا من البيانات التي كنا قادرين سابقًا على الحصول عليها حول أسماء النطاقات التي كان المستخدمون يستعلمون عنها أصبح الآن محجوبًا، ويرجع ذلك لأن نظام أسماء النطاقات أصبح يقدّم مستوى أعلى بكثير مما كان عليه سابقًا لحماية خصوصية المستخدمين. وهذا أمر جيد جدًا للإنترنت وللمستخدمين — لكنه ليس جيدًا بالضرورة للجهود التي تحاول فهم الصورة الكاملة.

وقد واجهنا تحديات مثيرة للاهتمام خلال العمل، لكننا تمكّنا من التعامل مع ما توفر لدينا من بيانات، ونجحنا في تحقيق الأهداف.

الهدف 1: ضمان القدرة على تقييم تضارب الأسماء. وفي هذا الإطار، قمنا بتطوير إطار عمل يعتمد على مستويات متصاعدة من التحليل والتفصيل، وذلك حسب درجة المخاطر المرتبطة بكل حالة من حالات تضارب الأسماء.

الهدف 2: توفير عملية تساعد ICANN على تقييم خطط التخفيف والمعالجة فيما يتعلق بحالات تضارب الأسماء المحددة. وقد اكتشفنا — أكثر من أي وقت مضى — أن كل حالة من حالات تضارب الأسماء فريدة إلى حدٍ ما، وتتطلب معالجات مخصّصة. الشريحة التالية من فضلك.

لن تكون هناك أي أسئلة امتحانية حول هذا الموضوع، ولكن هذا هو المخطط الذي ورد في التقرير ضمن الإطار الذي خلصت إليه الدراسة 2 لمشاريع تحليل تضارب الأسماء، والذي يأخذ في الاعتبار مخاطر تضارب الأسماء والتحديات المتطوّرة في رصدها والتخفيف من حدّتها.

أحد العناصر الرئيسية في هذا الإطار هو أننا نصّينا على وجود فريق مراجعة فنية يتولى الإشراف على العملية وإصدار أحكام مهنية حول المخاطر التي قد ترتبط بحالة معينة. وتمكّنا من افتراض أنه في العديد من الحالات لا تكون هناك مخاطر مستمرة.

فإمكانية التخفيف من المخاطر أو الوقاية منها قائمة، ولكن بما أنه لا توجد حالتان متطابقتان تمامًا، نفترض أن قدرًا معتبرًا من التقدير والخبرة سيكون مطلوبًا قبل التأكد من معالجة مخاطر تضارب الأسماء بالشكل المناسب. لذلك يعتمد جزء من هذا الإطار على وسائل

آلية، وجزء آخر يُحال إلى لجنة خبراء تشبه ما تستخدمه ICANN في سياقات أخرى حيث تكون المسائل معقدة ويُسهم عنصر التقدير في توجيه العملية. الشريحة التالية.

أما فوائد إطار تقييم مخاطر التضارب الذي قدّمته الدراسة 2 لمشاريع تحليل تضارب الأسماء للمجتمع، فهي أنه يوفّر إدارة استباقية للمخاطر من خلال تحديد مخاطر تضارب الأسماء والسماح بوضع ومراجعة استراتيجيات التخفيف قبل أن تتسبب في أي ضرر.

وقد عملنا بجهد على ضمان أن يكون الإطار متّسقًا وفعّالًا. فهناك نهج مركزي لبعض عمليات التحليل يضمن تقييمًا شاملاً للمخاطر وتخفيفها عبر جميع طلبات الحصول على نطاقات gTLD الجديدة، وذلك لأن مسؤولية منطقة الجذر تقع على عاتق ICANN.

كما أن الإطار قائم على البيانات، مما يمكّن من اتخاذ قرارات مستنيرة تضمن توسّعًا آمنًا في فضاء أسماء الإنترنت.

تمكنّا أيضًا من معالجة قدر كبير من مخاوف الخصوصية المرتبطة بهذا المجال من العمل. لأنه رغم أن تقييم تضارب الأسماء ينطوي بطبيعته على مخاطر، إلا أن أحد الأمور التي شددنا عليها هو أن عدم تقييم تضارب الأسماء بدقة يشكل خطرًا على الخصوصية، سواءً من خلال وصول البيانات الخاطئة إلى الأشخاص الخطأ أو وصول البيانات الصحيحة إلى الأشخاص الخطأ. وفي تقديرنا، فإن مخاطر الخصوصية الناتجة عن عدم التقييم الدقيق لتضارب الأسماء أكبر من المخاطر المرتبطة بعملية التقييم نفسها.

وبطبيعة الحال، تختلف كل حالة عن الأخرى، لكن امتلاك القدرة على إجراء تحليل مقارن للمخاطر بين اتخاذ إجراء ما وعدم اتخاذه يمنحنا أداة إضافية لتحليل هذه الحالات. لذلك نخلص إلى أن الكشف المبكر عن المخاطر والتخفيف المستند إلى معلومات كافية أمران ضروريان لأمن واستقرار نظام أسماء النطاقات.

هذا هو الملخص على المستوى العام. ويسعدني تلقي الأسئلة إذا سمح الوقت.

(MARCO HOGEWONING) ماركو هوغوونينغ: شكرًا لك يا سوزان. أقدر مساهمتك كثيرًا. وأنا أيضًا أعترف—وأقف مصحَّحًا إلى الأبد—بأني خلطتُ بين تضارب الأسماء وتشابه السلاسل. ولن أرتكب هذا الخطأ مرة أخرى. كما يسعدني للغاية رؤية الاستمرارية المؤسسية التي تقدّمها اللجنة الاستشارية للأمن

والاستقرار في هذا الموضوع على مرّ السنوات. أرى أن نيكو رفع يده. لدينا متّسع للإجابة عن سؤالٍ أو سؤالين. لا أرى أحدًا آخر في قائمة المتحدثين، لذا تفضّل يا نيكو.

(NICOLAS CABALLERO)
نيكولاس كاباليرو: أود فقط التعليق بشكلٍ سريع. إذا كان بإمكاننا العودة إلى الشريحة في الصفحة 23. نعم، ها هي. لدينا هناك أربع خطوات، وسؤالي يتعلق بالوقت. ما متوسط المدة المتوقعة؟ هل نتحدث عن أيام أم أسابيع أم أشهر؟ أريد فقط مقارنة ذلك مع 32 خطوة— تتذكرون عرض الأمس مع المنظمة الداعمة للأسماء العامة، أليس كذلك؟—من حيث الكفاءة والسرعة وغيرها من الجوانب. إذن، في المتوسط، كم من الوقت قد تستغرق هذه العملية؟

(SUZANNE WOOLF)
سوزان وولف: كان ذلك في الواقع سؤالاً ناقشناه كثيرًا، ولم نتمكن من التوصل إلى إجماع نهائي حول ما ينبغي التوصية به، لأنه، كما قلت، هناك ضغوط تدفع نحو جعل العملية سريعة قدر الإمكان، ولكننا في الوقت نفسه لا نريد أن نفوّت مخاطر مهمة. لذلك كنا نفكر في نطاق أسابيع وليس أشهرًا أو سنوات، لكن هذا في الحقيقة أمر اضطررنا لترك القرار النهائي بشأنه لفرق العمل والمجتمع.

(MARCO HOGEWONING)
ماركو هوغوونينغ: شكرًا لكم. لدينا متّسع من الوقت لأخذ سؤال آخر، لكنني لا أرى أي شخص في القاعة. لذا أودّ فقط أن أشكركِ يا سوزان على شرحكِ المفصّل. وكما ذكرتِ، ستكون الشرائح متاحة على الإنترنت.

(SUZANNE WOOLF)
سوزان وولف: نعم.

(MARCO HOGEWONING)
ماركو هوغوونينغ: يمكننا الانتقال إلى موضوعنا التالي. وهذا الموضوع طُرح في الواقع من قِبل المسؤولين عن موضوع انتهاك نظام أسماء النطاقات، الذين تساءلوا — بما أنّ لدينا الآن تقرير عن المشكلات — عمّا إذا كان بإمكانك يا رام، أنت وزملاؤك في اللجنة الاستشارية للأمن والاستقرار، مشاركة أي توصيات تقنية أو وجهات نظر حول تقرير المشكلات بعد نشره.

(RAM MOHAN)
رام موهان: شكرًا لك يا ماركو. قبل أن أجيب عن سؤالك، أردت أيضًا أن أَطلع اللجنة الاستشارية الحكومية على ما ورد في الشريحة السابقة بشأن عملٍ بدأناه مؤخرًا يرتبط بفضاء الأسماء. لقد بدأنا فريق عمل يُطلق عليه "الإدماج المسؤول في نظام أسماء النطاقات (RIDE)". وما نركّز عليه هو ما يحدث عندما تسعى المعرّفات الموجودة في فضاءات أسماء أخرى— وتحديدًا فضاء أسماء سلاسل الكتل—إلى الارتباط والتفاعل مع المعرّفات، وأسماء النطاقات، والأنظمة الموجودة ضمن نظام أسماء النطاقات. لقد بدأنا هذا العمل ونتوقع تقديم بعض التعليقات والاستنتاجات بشأنه.

نركّز تحديدًا على القضايا المتعلقة بدورة حياة اسم النطاق، والتباس المستخدمين، والاحتيال، وغير ذلك، وكذلك المخاطر المحتملة على أمن واستقرار نظام أسماء النطاقات التي قد تظهر عند وجود أنظمة في فضاءات أسماء أخرى تستخدم مصطلحات أو كلمات مشابهة لفضاء الأسماء الذي نعرفه، لكنها ليست مطابقة، رغم أنها قد تكون مرتبطة بها بطريقة ما. ما زلنا في بدايات هذا العمل، وسنواصل إطلاعكم على المستجدات.

وفي الشريحة التالية، وبالعودة إلى سؤالك يا ماركو، يسعدنا للغاية أن هناك ورقة سياسات قد بدأت—أو على الأقل هناك عمل بدأ بالفعل—حول انتهاك نظام أسماء النطاقات، وأن هناك عملية تطوير سياسات جارية بشأن هذا الموضوع. يمكنك الانتقال إلى الشريحة التالية.

في الماضي، كان ما تقوم به اللجنة الاستشارية للأمن والاستقرار هو تقديم التعليقات والنصائح بعد صدور توصيات السياسات. ونحن الآن بصدد تغيير هذا النموذج بالتعاون مع زملائنا في المنظمة الداعمة للأسماء العامة. ولقد دُعينا لتمثيلنا في عملية وضع السياسات نفسها.

لكن ما نقوم به ليس المشاركة في النقاشات حول ما إذا كان ينبغي أن يكون هناك مسار واحد أو مساران أو ثلاثة مسارات أو دمجها جميعًا، فهذه أمور يختص بها القائمون على وضع السياسات. ومع ذلك، نعتزم التدخّل للحديث عن المشكلات المحددة المتعلقة بالانتهاك، وملاحظاتنا حولها، خصوصًا أننا نقضي وقتًا طويلاً في دراسة تطوّر الانتهاك واتجاهاتها المستقبلية.

نولي تركيزًا كبيرًا على هذا المجال، إذ نعتقد أنه موضوع مهم، وفي نقاشاتنا مع مجلس إدارة ICANN حول أولويات عام 2026، على سبيل المثال، قمنا بتأييد بعض النقاط التي طرحتها المنظمة الداعمة للأسماء العامة والأطراف المتعاقدة، والتي تفيد بأن انتهاك نظام أسماء النطاقات يجب أن يكون ضمن أعلى الأولويات. دائمًا هناك قائمة من القضايا المتنافسة، لكن إذا لم نُحسن التعامل مع هذا الموضوع، وإذا أخفقنا فيه، فلن يتضرر المستخدمون فقط— بل ستتضرر سمعة نموذج أصحاب المصلحة المتعددين الذي نقدّمه جميعًا كأفضل مثال على التنظيم الذاتي الناجح. علينا أن نقوم بالأمور بالشكل الصحيح، ويجب أن يكون موضوع انتهاك نظام أسماء النطاقات محور تركيز أساسي.

لذلك نحن منخرطون بعمق في هذا العمل، ونسهم فيه، ونعتزم المشاركة بدرجة أكبر في مرحلة التصميم مقارنةً بما قمنا به في الماضي.

(MARCO HOGEWONING) ماركو هوغوونينغ: شكرًا لك يا رام، من الرائع سماع ذلك. وبما أن النقاش مفتوح بهذا الشكل، أتساءل ما إذا كان أي من العاملين في مجال مكافحة انتهاك نظام أسماء النطاقات يرغب في الرد على ما قيل. أو إذا كان هناك أي أسئلة إضافية موجهة إلى اللجنة الاستشارية للأمن والاستقرار حول هذا الموضوع؟ أو أي شخص آخر بالطبع لديه سؤال حول هذا الموضوع؟ يانوس، ممثل المفوضية الأوروبية، الكلمة لك.

(JANOS DRIENYOVSZKI) يانوس دراينوفسكي: شكرًا جزيلًا لكم مرة أخرى على حضوركم اليوم وعلى عروضكم التقديمية. ما نتساءل عنه فيما يتعلق بعمليات وضع السياسات هو أهمية تحديد النطاق الصحيح منذ البداية، لأننا سنبذل جهدًا كبيرًا في هذا المسار. ونتساءل عن آرائكم بشأن مسار التسجيل الجماعي —

لنسمّه كذلك — مسألة التسجيل الجماعي. لأن ما نريد تحقيقه هو أنه عند نهاية عملية وضع السياسات نصل إلى نتيجة فعّالة تستهدف بالفعل ما نريد استهدافه.

لقد ذكرنا واجهات برمجة التطبيقات، ولكن كنا نتساءل عمّا إذا كان النهج المطروح سيُغطي بشكلٍ كامل أغلب التقنيات أو الأدوات التي تُمكّن من عمليات التسجيل واسعة النطاق. لذلك سأكون ممتنًا للغاية لسماع آرائكم حول ما إذا كان هذا النهج مناسبًا، أو إذا كان ينبغي صياغة نطاق العمل بما يضمن أن يكون مستقبليًا ويأخذ في الاعتبار أي تطورات لاحقة. فهذا هو اهتمامي الشخصي، إذ لا أعلم ما هي التقنيات الأخرى التي قد توجد وتُمكّن هذا النوع من التسجيل الجماعي. شكرًا لكم.

(RAM MOHAN)
رام موهان:

شكرًا لكم. الإجابة هنا تحمل بعض التفصيل، لأن هناك حالات تكون فيها أسباب مشروعة لإجراء تسجيلات جماعية. على سبيل المثال: قد ترغب شركة ما في حماية منتج جديد فتقوم بتسجيل مئة نطاق دفعة واحدة. كما أن هناك تساؤلًا آخر: هل تتم التسجيلات عبر عدة نطاقات مستوى أعلى أم داخل نطاق واحد فقط؟ فهناك تفاصيل مختلفة في كل حالة.

وأود الإشارة إلى أن الوصول عبر واجهات برمجة التطبيقات ليس دائمًا الوسيلة الوحيدة للتسجيل الجماعي. فقد رأينا العديد من الحالات التي استخدم فيها أصحاب النوايا السيئة طرقًا غير معتمدة على واجهة برمجة التطبيقات للتسجيل الجماعي، كوسيلة للتمويه لأنهم يعلمون أن التسجيل عبر هذه الواجهات يخضع لمراقبة أكبر.

ومع ذلك، أرى أن هذا مجال جيد للبحث فيه. فمن الضروري وضع تعريف واضح لمفهوم التسجيل الجماعي. وأحد المخاوف التي نتشاركها مع آخرين في المجتمع هو أنه إذا وضعتم عتبة رقمية — كأن تقولوا إن أي تسجيلات أقل من رقم معيّن لن تخضع لنفس مستوى التدقيق — فسيتم التحايل على ذلك بلا شك. لذا، هناك عمل ينبغي القيام به في هذا الجانب.

آمل وضع سياسة توفّر إطارًا عامًا للسلوكيات التي نريد منعها، بدل التركيز على الأساليب المحددة التي تُرتكب بها تلك السلوكيات. وأعتقد أن هذا هو الفارق الذي ينبغي أن نستهدفه في عملية وضع السياسات.

(MARCO HOGEWONING)
ماركو هوغوونينغ:

شكرًا لك يا رام. لاحظت أن قائمة المتحدثين أصبحت شبه خالية، وهذا يمنحني فرصة للانتقال إلى النقطة التالية. ومجدّدًا، نقدر كثيرًا مداخلتك في هذه الجلسة. وكما ذكرتَ، ستكونون جزءًا من عملية وضع السياسات (PDP)، وذكرتم في مداخلتكم الافتتاحية أننا نقوم بتعزيز الروابط بين اللجنة الاستشارية الحكومية واللجنة الاستشارية للأمن والاستقرار. وهذا يقودنا إلى سؤال أوسع حول أين نرى فرصًا للتعاون. وستكون كل من اللجنة الاستشارية الحكومية واللجنة الاستشارية للأمن والاستقرار جزءًا من عملية وضع السياسات هذه، وقد لا يكون ذلك المسار الوحيد للمضي قدمًا.

رجاءً الانتقال إلى الشريحة التالية. أم أن هذا ما زال متعلقًا بانتهاك نظام أسماء النطاقات، كلامي موجه لممثل الهند؟ أم أن سؤالك يتعلق بهذه المسألة المطروحة تحديدًا؟ أرى أن يدك مرفوعة.

[ممثل الهند]:

فيما يتعلق بانتهاك نظام أسماء النطاقات بشكلٍ عام، ربما أرغب في معرفة رأي رام في هذا الشأن. فما التأثير المحتمل لتقليص فترة الأيام الخمسة عشر المخصّصة [للحفاظ على الدقة] على الحدّ من انتهاك نظام أسماء النطاقات؟ نحن نعتقد أنّها واحدة من أبسط الخطوات التي يمكن اتخاذها، ويمكن أن تُسهم بشكلٍ كبير في الحد من انتهاك نظام أسماء النطاقات ومواجهته.

ربما كان التحقق أو التوثيق الحقيقيّ يمثل تحديًا قبل عشر سنوات، لكن اليوم هذه الأمور تُنفّذ بسهولة. فنحن نقوم بها ثلاث أو أربع مرات يوميًا على الأقل. على سبيل المثال، عندما تسجّل دخولك إلى فندق، تحتاج إلى التوثيق. وعندما تدخل صالة مطار، تقوم بعملية التحقق والتوثيق. لذلك أتساءل فعلاً: كيف نسمح لشخص بالحصول على اسم نطاق دون أي عملية توثيق؟ علمًا بأننا لا نتحدث حتى عن "الهوية" بل عن مجرد "التحقق".

وبناءً على ذلك، أرغب في سماع آرائكم حول هذا الموضوع، لأنني أعتقد أنكم تُدركون جيّدًا المنطق وراء السؤال حول سبب وجود هذه العملية أصلاً.

(MARCO HOGEWONING)
ماركو هوغوونينغ: شكرًا لكم. إذن أفهم أن الموضوع يتعلق بفترة الأسبوعين المخصّصة لعملية التحقّق — أي فترة السماح البالغة أسبوعين، أليس كذلك؟ رام، هل لديك أي آراء حول هذا الإطار الزمني؟

(RAM MOHAN)
رام موهان: شكرًا جزيلاً. لقد سبق أن عبّرنا عن رأينا بشأن الطلبات العاجلة، وأعتقد أن الخلاصة هي أنه إذا وُصِف الطلب بأنه "عاجل"، فيجب فعلاً أن يعني ذلك شيئًا. ومن وجهة نظرنا، يعني ذلك أن الطلب يتطلّب استجابة سريعة للغاية، ولا ينبغي أن يشبه الأمر الاتصال بخدمات الطوارئ في الحياة الواقعية؛ فعندما تتصل بالطوارئ، لا تتوقع الحصول على رد بعد 15 يومًا أو بعد يومي عمل أو نحو ذلك. لذلك، من وجهة نظرنا، هذه النقطة تعد مهمّة.

وبالنسبة للسؤال المتعلّق بالتحقق والتوثيق، فمن جانب اللجنة الاستشارية للأمن والاستقرار، لا أعلم أننا قد توصّلنا إلى موقف موحّد يمثّل جميع أعضاء اللجنة بهذا الخصوص. ولكن نلاحظ أن باحثين في مجال الأمن وبعض جهات إنفاذ القانون قد ذكروا أنهم يشعرون بأنهم مقيّدون بسبب صعوبة الوصول إلى بعض معلومات المسجّل - المشترك بطريقة سهلة. ولذلك، كنا نشجّع على وضع أنظمة وصول متداخلة يمكنها تمكين الكشف عن هذه المعلومات للجهات التي لديها مصالح مشروعة للوصول إليها.

هذا هو موقفنا بشكلٍ عام. أمّا بالنسبة للطلبات العاجلة تحديدًا، فنحن نرى—وخاصة عندما تعمل كل من اللجنة الاستشارية الحكومية ومجلس الإدارة معًا—أنه ينبغي أخذ المعنى القاموسي لكلمة "عاجل" بعين الاعتبار، وألا يكون معيار "المعقول تجاريًا" هو الحدّ الأدنى المعتمد في هذا السياق. شكرًا لكم.

[ممثل الهند]: لا، لم يكن سؤالي متعلقًا بالطلبات العاجلة. سؤالي كان حول إمكانات الحدّ من انتهاك نظام أسماء النطاقات من خلال تقليص فترة 15 يومًا بين التحقّق أو التوثيق وبين تسجيل اسم النطاق. أعتقد أن هذا أمر يصعب عليّ استيعابه حقًّا في عصرنا الحالي.

(RAM MOHAN)
رام موهان:

نعم، شكرًا لك على التوضيح. مرة أخرى، لا أعتقد أنني أستطيع التحدث باسم اللجنة الاستشارية للأمن والاستقرار بأكملها. لكنني أرى أن هذا مجال يحتاج إلى دراسة معمّقة وجادة. ينبغي لنا النظر إلى الأضرار التي قد تلحق بالمستخدمين ومقارنتها مع المتطلبات التعاقدية الأخرى وعمليات وضع السياسات الجارية. وعليه، يجب أن نُبقي أضرار المستخدمين في مقدّمة أولوياتنا في هذا المجال.

(MARCO HOGEWONING)
ماركو هوغوونينغ:

شكرًا لك يا ممثل الهند. وأتوجه بالشكر لكلٍ من رام واللجنة الاستشارية للأمن والاستقرار. هل هناك أي أسئلة مُلِحّة أخرى؟ لدينا دقيقتان متبقيتان. ويسعدني أيضًا أن نبدأ في اختتام الجلسة ومنحكم استراحة لتناول القهوة. لذا دعوني أضيف، كما هو مذكور هنا: "إمكانيات التعاون المستقبلي". نيكو، هل تسمعني؟

(NICOLAS CABALLERO)
نيكولاس كاباليرو:

شكرًا لممثل هولندا. لدي سؤال أخير يتعلق بالتعاون في مجال البرامج مفتوحة المصدر. هل سيكون ذلك جزءًا من حزمة التعاون؟ وأطرح هذا السؤال لأنّه خلال منتدى حوكمة الإنترنت الأخير في النرويج، قامت حكومة النرويج بمشاركة حلول برمجية مفتوحة المصدر، وهناك أكثر من 45 دولة تستفيد حاليًا من ذلك. فما هي الآلية، في حال كان لدينا أي زميل من أعضاء اللجنة الاستشارية الحكومية مهتم بمعرفة كيفية التعاون في هذا المجال؟ ما الإجراءات الواجب اتباعها؟

(RAM MOHAN)
رام موهان:

أقترح أن يتواصلوا معي بصفتي الرئيس، أو مع فريق اللجنة الاستشارية للأمن والاستقرار المتميز لدينا. وسنقوم بتهيئة حوار يمكن من خلاله النظر في أفضل السبل التي نستطيع من خلالها تقديم المحتوى والدعم لكم، إضافةً إلى التعاون والعمل جنبًا إلى جنب معكم. فنحن مهتمون جدًا بهذا المجال، وهذا واحد من التقارير القليلة الصادرة عن اللجنة الاستشارية للأمن والاستقرار التي تستهدفكم أنتم تحديدًا، لذا ندعوكم للعمل معنا. نريد أن نجعل هذا التعاون مفيدًا لكم، وعندما تتعاونون معنا فإن ذلك يُثبت أن إنتاج هذا النوع من العمل هو جهد ذو قيمة بالنسبة لنا.

(MARCO HOGEWONING) ماركو هوغوونينغ: شكرًا لكم. وعلى هذه الملاحظة، أودّ أن أتقدّم بجزيل الشكر لكلٍ من رام وسوزان ومارتن وتارا على انضمامكم إلينا مرة أخرى. وفيما يتعلّق بموضوع هذه الشريحة، فإننا نتطلّع إلى مزيد من التعاون في المستقبل. وبهذا، ما لم تكن لديك أي تعليقات أخيرة يا نيكو، أعتقد أنه يمكننا الآن التوجّه لتناول القهوة.

(NICOLAS CABALLERO) نيكولاس كاباليرو: لا، فقط بعض الأمور التنظيمية. سنأخذ الآن استراحة لتناول القهوة. استمتعوا بقهوتكم. وسنعاود الاجتماع في الساعة 4:30. شكرًا جزيلاً. انتهت هذه الجلسة. شكرًا لك يا رام.

[نهاية التدوين النصي]