ICANN77 | منتدى السياسات – منظمة دعم أسماء النطاقات لرمز البلد ccNSO: المبادرات التشريعية التي تؤثر على نطاق المستوى الأعلى لرمز البلد
الثلاثاء، الموافق 15 يونيو/حزيران 2023 – من الساعة 10:45 إلى الساعة 12:15 بالتوقيت الرسميّ الشرقي لأمريكا الشمالية

كلوديا رويز: أهلًا ومرحبًا بكم في جلسة المبادرات التشريعية التي تؤثر على نطاق المستوى الأعلى لرمز البلد لمنظمة دعم أسماء النطاقات لرمز البلد ccNSO. معكم كلوديا رويز وزميليّ، بارت بوسوينكل وكيمبرلي كارلسون، سنكون مديري المشاركة عن بُعد لهذه الجلسة. يُرجى العلم بأنه يجري تسجيل هذه الجلسة وتحكمها معايير السلوك المتوقعة في مؤسسة ICANN. خلال هذه الجلسة، ستتم قراءة الأسئلة أو التعليقات المقدمة في الدردشة بصوت عالٍ فقط إذا تم وضعها بالشكل المناسب كما أشرت في الدردشة. سأقرأ الأسئلة والتعليقات بصوتٍ عالٍ خلال الوقت الذي حدده منسق أو رئيس الجلسة. تشمل الترجمة الفورية لهذه الجلسة الإسبانية والفرنسية والعربية. يُرجى النقر فوق أيقونة الترجمة الفورية في برنامج Zoom وتحديد اللغة التي ستستمعون إليها أثناء هذه الجلسة. عند الرغبة في التحدث، يُرجى رفع اليد في غرفة Zoom. وبمجرد أن ينادي منسق الجلسة اسمك، يُرجى إلغاء كتم صوت الميكروفون وأخذ الكلمة. وقبل التحدث، تأكدوا من تحديد اللغة التي ستتحدثون بها من قائمة الترجمة الفورية. ويُرجى التكرم بذكر اسمك للتدوين في السجل وتحديد اللغة إذا كنتم ستتحدثون بلغة أخرى غير الإنجليزية. وعند التحدث يتعين التأكد من كتم صوت جميع الأجهزة والإشعارات الأخرى. ويُرجى التحدث بوضوح وبسرعة معقولة للسماح بالترجمة الفورية الدقيقة. تتضمن هذه الجلسة تدوينًا آنيًا للحوار بصورة آلية. ويُرجى العلم بأن هذه النسخة النصية ليست رسمية أو موثوقة. لعرض التدوين الآني للحوار، يُرجى النقر فوق زر التسمية التوضيحية المغلقة في شريط أدوات برنامج Zoom. ولضمان شفافية المشاركة في نموذج أصحاب المصلحة المتعددين في مؤسسة ICANN، نطلب منكم تسجيل الدخول إلى جلسات Zoom باستخدام الاسم الكامل. على سبيل المثال، الاسم الأول واسم العائلة أو اللقب. فقد يتم إقصاؤك من الجلسة في حالة عدم تسجيل الدخول بالاسم بالكامل. شكراً لك. وبذلك، أعطي الكلمة إلى أناليز ويليامز. شكراً لك.

أناليز ويليامز: شكراً لك. مرحبًا جميعًا وشكرًا لكم على انضمامكم إلينا في جلسة منظمة دعم أسماء النطاقات لرمز البلد ccNSO الجديدة هذه، والتي تنظمها لجنة منسقي علاقات حوكمة الإنترنت في منظمة دعم أسماء النطاقات لرمز البلد ccNSO. معكم أناليز ويليامز. أنا من إدارة نطاق au. ورئيس لجنة منسقي علاقات حوكمة الإنترنت. تتناول جلستنا الجديدة اليوم المبادرات التشريعية المتعلقة بالأمن السيبراني وكيفية تأثيرها على نطاق المستوى الأعلى لرمز البلد. لدينا اليوم متحدثون من دولة كندا، وفانواتو، وموزامبيق وكوستاريكا، وسلوفينيا. لقد طُلب من كل مقدمينا النظر في المبادرات التشريعية للأمن السيبراني التي تؤثر على نطاق المستوى الأعلى لرمز بلدهم أو منطقتهم، وما إذا كان نطاق المستوى الأعلى لرمز البلد الخاص بهم قادرًا على التأثير على تطوير أو تنفيذ هذا التشريع، وماذا فعلوا لإدارة تأثير هذه المبادرات. سيتم تخصيص 15 دقيقة لكل متحدث لعرضهم التقديمي، والتي تتضمن وقتًا لأسئلة الجمهور. لذلك سنلتزم بهذا الوقت حتى يحصل كل متحدث على الوقت المخصص له. ولكن إذا كان هناك أي وقت إضافي في نهاية الجلسة، فسأفتح المجال لمزيد من التعليقات أو الأسئلة. نذكركم مُجددًا بأن لدينا ترجمة فورية متاحة لهذه الجلسة. إذن، هل لي أن أطلب من كل متحدثينا التحدث ببطء ووضوح حتى يتمكن المترجمون الفوريون من مواكبة ما يقولون؟ اسمحوا لي الآن أن أقدم المتحدث الأول وهي سابرينا ويلكيسون. سابرينا هي مديرة السياسات والبرامج في هيئة تسجيل الإنترنت الكندية. وهي حاصلة على درجة الدكتوراه في الإعلام والاتصالات وقامت بقيادة مجموعة من المشاريع البحثية في مجالات السياسة الرقمية والصحافة والنوع الاجتماعي. إليك الكلمة. شكرًا لك، سابرينا.

سابرينا ويلكنسون: شكرًا لك، أناليز. تسرني رؤيتكم جميعاً اليوم. اليوم، أود أن أتحدث إليكم عن آراء هيئة تسجيل الإنترنت الكندية ومشاركتها بجزء كبير من تشريعات الأمن السيبراني الفيدرالية المحلية أو بجزء مقترح من تشريعات الأمن السيبراني الفيدرالية المحلية تسمى مشروع القانون C-26 والذي يتم إمراره حاليًا في العملية التشريعية الكندية. وعلى وجه الخصوص، سأركز على الجزء الثاني من مشروع القانون. لننتقل إلى الشريحة التالية، رجاءً.

في العرض التقديمي الذي بين يدينا اليوم، أريد أن أقوم بثلاثة أمور رئيسية. أولًا، أود أن أخبركم بما تم اقتراحه بالضبط في الجزء الثاني من مشروع القانون الذي تتعامل معه هيئة تسجيل الإنترنت الكندية. وأود أن أخبركم كيف شاركت هيئة تسجيل الإنترنت الكندية في هذا الحوار

حول مشروع القانون C-26 حتى الآن، سواء في تطوير مواقف السياسة العامة أو الدفاع عنها. وأود أيضًا أن أتطرق إلى كيف تخطط هيئة تسجيل الإنترنت الكندية لمواصلة المشاركة بشكل مستمر. لننتقل إلى الشريحة التالية، رجاءً.

إذن، فمشروع القانون C-26 يتكون من جزأين رئيسيين. سأركز على الجزء الثاني لأنه هو العنصر الذي تتعامل معه هيئة تسجيل الإنترنت الكندية من مشروع القانون. وما سيفعله هذا القانون المقترح باختصار، والذي إذا تم تمريره، فسيُطلق عليه قانون حماية الأنظمة الإلكترونية الحرجة. ما سيفعله هو أنه سيُطبق أولًا على المشغلين الخاضعين للتنظيم الفيدرالي في أربعة قطاعات بنية تحتية مهمة محددة، وهي الاتصالات والبنوك والطاقة والنقل. مما سيسمح للحكومة بوضع متطلبات على المشغلين المعينين ضمن هذه القطاعات الأربعة الخاضعة للتنظيم الفيدرالي لضمان اتخاذهم خطوات بعينها حول الأمن السيبراني، وتطوير برامج الأمن السيبراني، على سبيل المثال: الإبلاغ عن بعض أحداث الأمن السيبراني التي قد تحدث، والاحتفاظ بسجلات محددة في عالم الأمن السيبراني أيضًا. سيضع القانون المقترح أيضًا لوائح، ويمنح الحكومة سلطة إصدار أوامر للمشغلين المعينين في إطار هذه القطاعات الأربعة لاتخاذ خطوات معينة لمعالجة أي حادث سيبراني، على سبيل المثال. كما أنه يحدد عددًا من سلطات إنفاذ القانون للحكومة في الحالات التي لا يتم فيها اتخاذ هذه الخطوات أو في حال عدم استيفاء هذه المتطلبات. لننتقل إلى الشريحة التالية، رجاءً.

فلماذا يعتبر مشروع قانون C-26 مهمًا لهيئة تسجيل الإنترنت الكندية؟ لماذا نهتم بمشروع قانون C-26؟ ولماذا نشارك في حوار السياسات المستمر هذا؟ لعدة أسباب مختلفة. أولًا، مشروع قانون C-26 لديه الإمكانات المناسبة، والجزء الثاني منه لديه القدرة على جذب مجموعة واسعة من المشغلين بخلاف الموضحين حاليًا في مشروع القانون. بالإضافة إلى ذلك، تتوافق أهداف الجزء الثاني مع... إن أهداف القانون المقترح، والتي تتمثل في رفع مستوى خط الأساس للأمن السيبراني على نطاق واسع عبر البنية التحتية الحيوية، تتماشى مع مهمة هيئة تسجيل الإنترنت الكندية لبناء إنترنت موثوق به للكنديين.

هناك أيضًا فرصة لهيئة تسجيل الإنترنت الكندية للمشاركة في تحسين مشروع القانون. إذ لا يقتصر الأمر على أن مشروع القانون ذا صلة بنا كمشغلين ويتماشى مع مهمتنا المتمثلة في بناء إنترنت موثوق به، ولكننا نرى أن هناك مساحة لنا حتى يكون لنا تأثير إيجابي هادف على أحكام معينة في مشروع القانون. ولأننا موجودون في أوتاوا، عاصمة كندا، فنحن أيضًا قريبون جدًا

جغرافيًا من المساحات التي يتم فيها اتخاذ القرار حول تعديل أو تطوير مشروع القانون في الوقت الحالي.

أخيرًا، نحن نرى أيضًا المشاركة في حوار السياسة حول مشروع قانون C-26 كقيادة فكرية وفرصة للتوعية بمنتجنا. وأعني بذلك أنها مساحة يمكن أن تساهم فيها هيئة تسجيل الإنترنت الكندية بشكل هادف كمشغل تقني يتمتع بالخبرة ذات الصلة بالأمن السيبراني والقضايا الأخرى ذات الصلة الموضحة في مشروع القانون. وهي أيضًا فرصة لعرض منتجاتنا كمزود للأمن السيبراني. الشريحة التالية. شكراً لك.

لذا عند مراجعة مشروع القانون، صادفت هيئة تسجيل الإنترنت الكندية عددًا من المخاوف. فبينما نتوافق على نطاق واسع مع الأهداف الموضحة في الجزء الثاني من مشروع القانون C-26، فإن هناك مجالات نرى فيها مساحة للتحسين. وهذا هو الأساس الذي ننخرط لأجله، أو هذه هي مواقف السياسة التي نحددها عندما نكون في الاجتماعات أو نجري مناقشات حول الجزء الثاني من مشروع قانون C-26. على مستوى عالٍ جدًا، تتعلق هذه الاهتمامات بثلاثة مجالات أو قضايا رئيسية. لدينا مخاوف بشأن الرقابة.

كما ذكرتُ سابقًا، يمنح مشروع القانون C-26 الحكومة سلطات واسعة جدًا، لا سيما من حيث تمكينها، حيث يسمح للحكومة بإصدار أوامر للمشغلين المعينين بموجب القانون باتخاذ خطوات معينة فيما قد يكون حالة طارئة في الغالب. لدينا مخاوف بشأن بعض أحكام الرقابة الحالية المتعلقة بتلك السلطة، لكنها محدودة إلى حد ما.

لدى هيئة تسجيل الإنترنت الكندية أيضًا مخاوف بشأن مشاركة المعلومات، نظرًا لكمية المعلومات التي سيتم جمعها بموجب مشروع القانون أو القانون، إذا ما كان سيصبح قانونًا، ومدى مشاركة هذه المعلومات بين مجموعة واسعة من الأطراف. وأخيرًا، لدى هيئة تسجيل الإنترنت الكندية بعض المخاوف بشأن الشفافية. نحن ندرك بالتأكيد أنه في مسائل الأمن السيبراني، السرية إلى حد ما ضرورية ومهمة. ومع ذلك، نعتقد أن هناك مساحة لمزيد من الشفافية التي من شأنها أن تعطي معلومات للكنديين وكذلك المشغلين المعينين حول كيف تُستخدم تلك التوجيهات الموجهة للمشغلين المعينين على وجه الخصوص. لننتقل إلى الشريحة التالية، رجاءً.

واستجابةً لهذه المخاوف الثلاثة، فإننا نقدم ثلاث توصيات ذات صلة. على مستوى عالٍ جدًا في مناصرتنا أو مشاركتنا في مشروع قانون C-26، فنحن نطلب إضافة آلية إشراف إضافية إلى عملية إصدار توجيهات الأمن السيبراني. نقترح أن تقتصر مشاركة المعلومات بموجب هذا القانون المقترح على أغراض محددة فقط، لأنه من وجهة نظرنا هناك بعض الغموض حول مدى مشاركة المعلومات التي تم جمعها بموجب القانون. وأخيرًا، نحن ندعو إلى نشر تقارير شفافية سنوية والتي من شأنها أن تزود الكنديين وكذلك المشغلين المعينين بمزيد من المعلومات حول كيفية استخدام الحكومة للتوجيهات التي بوسعها استخدامها في حالات معينة. لننتقل إلى الشريحة التالية، رجاءً.

ومع هذه التوصيات الثلاث، والتي تحيلنا إلى سلسلة من التعديلات التشريعية المقترحة، لدينا مخاوف متنوعة. كيف تعاملنا بالضبط مع من يتخذون القرارات حول كيفية تطوير مشروع القانون أو تعديله في خضم العملية التشريعية، ومن كنا نتعامل معهم، وإلى أي مدى كان هذا ناجحًا؟

بشكل عام، كان لدينا ثلاثة أنواع من الأنشطة الرئيسية أو مجالات المشاركة، إن صح التعبير. أولًا، عقدنا مجموعة من الاجتماعات مع صانعي القرار وأصحاب المصلحة الآخرين. والتقينا بممثلين آخرين يشاركون في هذا الحوار حول مشروع قانون C-26 وكيف ينبغي تحسينه. والتقينا بصناع القرار أو أولئك الذين يدعمون صناع القرار، مثل الموظفين السياسيين. والتقينا أيضًا بعدد من الموظفين الحكوميين رفيعي المستوى الذين يشاركون في تطوير مشروع القانون، والذين شاركوا في تطوير هذا التشريع، والذين يعملون على نطاق واسع في مجالات الأمن السيبراني والبنية التحتية الحيوية.

وشاركنا أيضًا علنًا في مساحات مثل هذه، وكذلك في لجنة عامة في مؤتمر اتصالات كندي كبير، حيث تمكنا من مشاركة وجهات نظرنا بصفتنا هيئة تسجيل الإنترنت الكندية، وكذلك الانخراط مع الآخرين الذين يشاركون في هذا النقاش، والذين لديهم خبرة في هذا المجال. وقمنا أيضًا ببعض الكتابات العامة حول وجهات نظرنا بشأن السياسات، وإلى أي مدى نعتقد أنه ينبغي دمجها في القانون. لننتقل إلى الشريحة التالية، رجاءً.

إذن، كيف نخطط لمواصلة المشاركة بينما يستمر مشروع القانون هذا في التحرك خلال العملية التشريعية؟ الآن، مشروع القانون في ما يسمى بمرحلة اللجنة. لذا، فإن مشروع القانون ينتظر

أن تتم مراجعته من قبل مجموعة من البرلمانيين الذين يدرسون مسائل السلامة العامة والأمن القومي. وسنستمر في مراقبة تقدم مشروع القانون عن كثب حيث ينتقل نوعًا ما إلى مرحلة اللجنة هذه ويخضع للمراجعة من قبل هؤلاء البرلمانيين، بالإضافة إلى الشهود الخبراء الآخرين. سنواصل الاجتماع مع صانعي القرار وأصحاب المصلحة الذين يشاركون في هذا النقاش لمشاركة آراء هيئة تسجيل الإنترنت الكندية وللفهم بشكل أفضل كيف تفكر الأطراف الأخرى وما الذي وارء دوافعهم ورؤاهم. وسنستمر أيضًا في الدفاع علنًا عن آراء هيئة تسجيل الإنترنت الكندية بشأن الجزء الثاني من مشروع قانون C-26 على وجه الخصوص في المنتديات العامة، مثل المساحات الدولية، كهذا، وكذلك في الأماكن المحلية أيضًا.

آمل أن أكون قد أعطيتكم اليوم لمحةً عن شكل هذا القانون، أو هذا القانون المقترح على مستوى عالٍ، وكيف تشارك هيئة تسجيل الإنترنت الكندية حتى الآن وكيف يبدو الأمر بالضبط، وأيضًا كيف نخطط لمواصلة المشاركة المستمرة. وستسرني الإجابة عن أية أسئلة.

أناليز ويليامز: شكرًا جزيلًا يا سابرينا. أيوجد أسئلة لـ "سابرينا"؟ نعم، من فضلك، شون.

شون كوبلاند: بالطبع، لدي سؤال لكِ. إحقاقًا للحق، شون كوبلاند، يعمل لصالح المركز القومي للمعلوماتية في جزر العذراء الأمريكية، لكن بصفتك مواطنًا كنديًا، كيف تم استقبال موقفك تجاه الرقابة؟

سابرينا ويلكنسون: شكرًا يا سيون. أود أن أقول إن جميع توصياتنا قد لقيت استحسانًا من صانعي القرار، وكذلك أصحاب المصلحة الذين التقينا بهم. فيما يتعلق بآلية الرقابة على وجه الخصوص، حاولنا جاهدين تحقيق هذا التوازن بين توفير مستوى إضافي من الإشراف، مع الحفاظ أيضًا على مستوى من السرعة والسرية، لأننا ندرك أهمية هذا في مسائل السلامة العامة والأمن القومي. أظن وآمل أننا حققنا هذا التوازن المناسب، وأعتقد أن ردود الفعل الإيجابية التي تلقيناها تشير إلى نجاحنا في هذا. شكراً لك.

أناليز ويليامز: شكرًا لك، سابرينا. أية أسئلة أخرى؟ لا أرى أي أسئلة، لننتقل إلى المتحدث التالي إذن. المتحدث التالي هو نورمان واربوت. نورمان هو مدير تقنية المعلومات والإتصالات وحوكمة الإنترنت في الجهة المنظمة للاتصالات السلكية واللاسلكية والبث الإذاعي في فانواتو. تفضل، نورمان.

نورمان واربوت: شكرًا لكم، ومرة أخرى، صباح الخير على كل من في الغرفة. ليلة سعيدة وأمسية طيبة على المشاركين عن بعد. اسمي نورمان واربوت، وأنا مدير تقنية المعلومات والاتصالات بهيئة الاتصالات في فانواتو، وهي أيضًا المالك المفوض لنطاق المستوى الأعلى لرمز البلد .vu. لننتقل إلى الشريحة التالية، رجاءً.

في عرضي التقديمي هذا الصباح، سأناقش بشكل أساسي بعض المبادرات التي عملنا عليها بالتعاون مع حكومة فانواتو، وكذلك دورنا كمدير ومسؤول لنطاق المستوى الأعلى لرمز البلد .vu. باختصار، نبذة حول هيئة الاتصالات السلكية واللاسلكية في فانواتو. هي هيئة قانونية تعمل بشكل مستقل عن الحكومة. لذلك، ليس لدينا أي مجلس إدارة، وليس لدينا أي لجنة. لدينا الجهة المنظمة والموظفون. لذا، فإن جميع القرارات تقع بالكامل على عاتق الجهة المنظمة. لدينا وظائف وصلاحيات عامة لتنظيم قطاع الاتصالات، وكذلك قطاع البث المباشر. تقدم الجهة المنظمة تقاريرها إلى رئيس الوزراء، كما تقدم المشورة للحكومة بشأن سياسات تقنية المعلومات والإتصالات من المصلحة الوطنية. لننتقل إلى الشريحة التالية، رجاءً.

إن نطاق .vu هو نطاق للنطاقات المستوى الأعلى في بلدنا، ويديره مكتب جهة تنظيم الاتصالات. في البداية، كان نطاق المستوى الأعلى لرمز البلد الخاصة بنا تديره شركة الاتصالات الخاصة بنا في التسعينيات. لذلك، عند إنشاء مكتب الجهة المنظمة، يتطلب القانون من مكتب الجهة المنظمة إدارة هذا المورد وتدبيره. قمنا بالانتقال من شركة اتصالات فانواتو في عام 2017، وأكملنا ذلك بنجاح في يناير 2020. لننتقل إلى الشريحة التالية، رجاءً.

ومن حيث أمان الإنترنت، عندما خططنا للانتقال، فقد وافق مكتب الجهة المنظمة على GoDaddy باعتباره مشغل السجل لنطاق المستوى الأعلى لرمز البلد .vu. لذلك، يبدأ مشغل السجل في تقديم الخدمة التي تلبي أفضل الممارسات الدولية وممارسات مؤسسة ICANN. لقد طورنا بعض السياسات لنطاق المستوى الأعلى لرمز البلد الخاص بنا، وقمنا أيضًا بتطوير لائحة

أسماء النطاقات التي تم الانتهاء منها في عام 2016. حاليًا، لدينا 34 أمناء سجل دوليين و5 محليين، وحتى الآن يلتزمون بمعايير الأمان الدولية المطلوبة التي وضعها مشغل السجل. لننتقل إلى الشريحة التالية، رجاءً.

كما يدعم مكتب الجهة المنظمة الحكومة ويساعدها في صياغة قانون الجرائم الإلكترونية. لدينا لائحة لحماية المستهلك تسمح لنا بإبلاغ المستهلكين بمخاطر أمن الإنترنت، وحماية الأطفال. تم الانتهاء من القانون، وتم تمريره عبر برلماننا الوطني، و[تمت مناقشته] في عام 2021. لننتقل إلى الشريحة التالية، رجاءً.

إحدى المبادرات التي نعمل عليها مع الحكومة بالتعاون مع مكتب المسؤول التنفيذي لمعلومات الحكومة، هي إنشاء فريق الإستجابة لحالات طوارئ الحاسب الآلي الخاص بنا CERT. تم إنشاء المكتب في عام 2018، وما زال يعمل حاليًا. لننتقل إلى الشريحة التالية، رجاءً.

وهناك مبادرة أخرى تتمثل في إنشاء حوكمة الإنترنت في فانواتو. نحن نساعد الحكومة أيضًا، وذلك بعد أن استضافت فانواتو المنتدى الإقليمي لحوكمة الإنترنت لمنطقة آسيا والمحيط الهادئ هنا في عام 2018. لذا، فإن هذا المكتب هو في الأساس منصة لأصحاب المصلحة المتعددين تسهل المناقشات حول السياسة العامة والقضايا. لذلك، يدعمه مكتب الجهة المنظمة ومكتب المسؤول التنفيذي لمعلومات الحكومة. لننتقل إلى الشريحة التالية، رجاءً.

لقد قمنا أيضًا بتطوير لائحة تسجيل بطاقات SIM. وهي في الأساس تعليمات من المكتب الوطني لإدارة الكوارث، وتستند إلى قرار مجلس الوزراء بأن يكون لدينا لائحة لتسجيل جميع بطاقات SIM وتخصيص هوية وطنية صالحة لكل بطاق. تم الانتهاء من هذه اللائحة. وهي الآن في السوق. جميع مزودي خدمة الإنترنت وخاصة شركتي الهاتف المحمول الرئيسيتين، يستخدمون ذلك لتسجيل بطاقة SIM. وهذا في الأساس إجراء للأمن السيبراني، ويضيف قيمة إلى مبادرات الأمن السيبراني في الدولة. لننتقل إلى الشريحة التالية، رجاءً.

لدينا عدد قليل من المبادرات التشريعية الوطنية التي ساعدنا بها الحكومة أيضًا، بالتعاون مع مكتب المسؤول التنفيذي لمعلومات الحكومة. في الوقت الحالي، نحن بصدد تقديم مشاريع القوانين هذه إلى برلماننا الوطني، ونأمل أن نحصل على بعض التحديثات في هذا الشأن في نوفمبر من هذا العام. ومع ذلك، في هذا التشريع الوطني، لدينا مشروع قانون للاتصالات الرقمية الضارة

ومشروع قانون لحماية البيانات والخصوصية والموهبة والحماية. إذن، هذه هي تدابير الأمن السيبراني، والتي تضيف أيضًا قيمة إلى مبادراتنا الوطنية للأمن السيبراني في الدولة. لننتقل إلى الشريحة التالية، رجاءً.

مرة أخرى، لقد شاركنا كثيرًا في توعية المجتمع. لدينا لائحة لحماية المستهلك، وكذلك لائحة تسجيل بطاقات SIM. لذلك، من المهم إبلاغ مستخدمينا، خاصةً بشأن فوائد ومخاطر استخدام الإنترنت، وأهمية هذه اللائحة، وكيف ستؤثر على المستهلك. وهذا جزء من برنامج التوعية لدينا على مدار العام. كما شاركنا أيضًا مع المدارس والمجتمعات وبالتعاون مع إدارة الإنترنت في فانواتو [IGF] وأصحاب المصلحة الآخرين لتعزيز الوعي في جميع أنحاء البلاد. لننتقل إلى الشريحة التالية، رجاءً.

أعتقد أن هذا كل ما لدي. شكراً لك. شكرا لكم جميعا على الاستماع.

أناليز ويليامز: شكرًا لك، نورمان. أيوجد أسئلة لـ "نورمان"؟ لدي سؤال، يا نورمان، إذا كنت لا تمانع. أعلم أنك لم تكن مسؤولًا بشكل مباشر بصفتك الجهة المنظمة، لكن فانواتو تعرضت مؤخرًا لهجوم سيبراني كبير جدًا. هل لديك أي آراء حول كيفية تأثير ذلك على مكتبك؟

نورمان واربوت: شكرًا على السؤال. نعم، حقيقةً، ليس لدي أي معلومات مفصلة عن هجوم الفدية العام الماضي. ومع ذلك، فهو هجوم من برمجيات الفدية، وأعتقد أن المتسللين اخترقوا أحد الخوادم [غير مسموع]. لذلك، تعين على فريق الحكومة إغلاق الخادم لأخذ المتسلل بعيدًا، ثم قاموا بإغلاق النظام. ولكن بشكل أساسي، من منظور نطاق المستوى الأعلى لرمز البلد .vu، ليس لدينا أي تأثير كبير عليه. ومع ذلك، تعين على الحكومة قطع اتصال الكثير من الخدمات عبر الإنترنت فقط للتأكد من إعادة بناء الخادم واستعادة جميع البيانات من النسخة الاحتياطية.

لذا، أعتقد أن التأثير الذي رأيته هو عملية الدفع، والضوابط [الحدود]، والمواقع الإلكترونية، والبريد الإلكتروني. وتعين على الحكومة إزالة هذه الخدمات من أجل إصلاح هذه المشكلة. أعتقد أن هذا كل ما يمكنني تقديمه عن الأمر. شكراً لك.

أناليز ويليامز: شكرًا لك، نورمان. أية أسئلة أخرى؟ نعم، أنجيلا، من فضلك.

أنجيلا: طاب صباحكم جميعًا. أنجيلا، بالمناسبة، أردت أن أسأل عما إذا كانت هناك أي لوائح محددة تتحدث عن الراديو عبر الإنترنت؟ عادة، يكون لديك ذلك في البث المباشر، ربما سياسات وأشياء من هذا القبيل، لكن هل تعاملونها بشكل مختلف لأن لديكم الآن راديو يعمل على مساحة النطاق؟ هل يعني ذلك إذن أن سياسات نطاق المستوى الأعلى لرمز البلد التي تتحدث عن إساءة الاستخدام تتحدث أيضًا عن محتوى الراديو الذي يتم تشغيله على إحدى منصات النطاق؟ شكراً لك.

نورمان واربوت. شكراً لك. بالنسبة لمكتب جهة التنظيم، من حيث منظور المحتوى، فنحن لا ننظم المحتوى. نحن ننظم خدمة الاتصالات فقط ونراقب السوق، لكننا لا ننظم أي محتوى سواء من أي موقع ويب للمحتوى أو أي شيء يأتي من البث المباشر. نحن لا ننظم المحتوى. أتمنى أن أكون قد أجبت على السؤال. شكراً لك.

أناليز ويليامز: شكرًا، نورمان. هل توجد أي أسئلة أخرى؟ لا أسئلة في الغرفة ولا أعتقد أنه ثمة أي منها على الإنترنت. لذلك، قد ننتقل الآن إلى المتحدث التالي الذي ينضم إلينا عبر الإنترنت عن بُعد. لدينا لورينو شيمان. يشغل لورينو حاليًا منصب رئيس هيئة تنظيم تقنية المعلومات والإتصالات في موزمبيق، والمعهد الوطني لتقنية المعلومات والاتصالات. في السابق، كان مستشارًا لتكنولوجيا المعلومات والاتصالات لوزير العلوم والتكنولوجيا والتعليم العالي، كما شغل سابقًا منصب الرئيس التنفيذي لشبكة موزمبيق للبحث والتعليم. تفضل، لورينو. شكراً لك.

لورينو شيمان: شكرًا لكم على إتاحة الفرصة لنا. اسمي لورينو شيمان من موزمبيق سأشارككم ما نقوم به في موزمبيق في مجال الأمن السيبراني والمبادرة التشريعية المتعلقة بنطاق المستوى الأعلى لرمز

البلد. نحن نمثل المعهد الوطني لتقنية المعلومات والإتصالات. وهو الجهة المنظمة للخدمة الرقمية في موزمبيق. لننتقل إلى الشريحة التالية، رجاءً.

هذه هي الموضوعات التي سيتم تغطيتها. مقدمة موجزة، وتفويض واختصاص المعهد الوطني لتقنية المعلومات والاتصالات، وإدارة نطاق المستوى الأعلى لرمز البلد الموزمبيقي، والتشريعات المعتمدة، وسياسة واستراتيجية الأمن السيبراني الوطنية، وإجراءات المتابعة، وتطوير الأطر القانونية الجديدة، وخاتمة موجزة. لننتقل إلى الشريحة التالية، رجاءً.

لذلك، تم إنشاء المعهد الوطني لتقنية المعلومات والاتصالات بمرسوم في عام 2011، ولكن تم تعديل هذا المرسوم في عام 2020. وهذا يعني أن المعهد الوطني لتقنية المعلومات والاتصالات هي الجهة المنظمة لتقنية المعلومات والاتصالات في موزمبيق. إنه مؤسسة وطنية عامة تتمتع بشخصية اعتبارية واستقلال إداري كمنظم لتقنية المعلومات والاتصالات في الدولة. ويشرف عليه الوزير المشرف على مجال تقنية المعلومات والاتصالات، وحاليا في الحكومة الحالية وزير العلوم والتكنولوجيا والتعليم العالي. لننتقل إلى الشريحة التالية، رجاءً.

كجزء من تفويض المعهد الوطني لتقنية المعلومات والاتصالات، فإنه يتضمن تطوير مقترح لمعايير السياسة واللوائح التي تضمن أمن وسلامة أنظمة تقنية المعلومات وتشغيلها ضد إساءة الاستخدام والانتهاك المحتملين. ونذكر أيضًا صراحة أنه يتعين على المعهد الوطني لتقنية المعلومات والاتصالات ضمان حوكمة الإنترنت في موزمبيق. لننتقل إلى الشريحة التالية، رجاءً.

من مجالات التفويض المحددة: ضمان تشغيل وإدارة نطاق المستوى الأعلى لرمز البلد الموزمبيقي، وهو نطاق .mz، إلى جانب العمل أيضًا في مجالات أخرى مثل الشهادة الرقمية لموزمبيق، وكذلك تسجيل المشغلين الرقميين ومقدم الخدمة الوسيط. لننتقل إلى الشريحة التالية، رجاءً.

بالنسبة لنطاق المستوى الأعلى لرمز البلد، ولا سيما نطاق .mz، أود مشاركة تاريخ موجز. تم إنشاء نطاق .mz في عام 2015، وتديره جامعة إدواردو موندلين، وهي مؤسسة أكاديمية سجلت نفسها. ولكن بعد الموافقة على قانون المعاملات الإلكترونية في عام 2017، تم إنشاء المعهد الوطني لتقنية المعلومات والاتصالات ككيان مسؤول عن إدارة نطاق المستوى الأعلى لرمز البلد الموزمبيقي. ونحن الآن بصدد العمل مع الجامعة لنقل جزء من أدوار ومسؤوليات نطاق المستوى

الأعلى لرمز البلد إلى المعهد الوطني لتقنية المعلومات والاتصالات. لكننا نترك جميع العمليات الفنية للجامعة بسبب تاريخهم في تشغيل نطاق .mz في موزمبيق. لننتقل إلى الشريحة التالية، رجاءً.

هناك العديد من اختصاصات المعهد الوطني لتقنية المعلومات والاتصالات في القانون، ولكن كان من بينها تقديم تعليمات واضحة لتطوير لائحة استخدام نطاق .mz. لقد قمنا بهذا العمل، وتمت الموافقة على هذه اللائحة في عام 2020 والتي أشارت إلى عملية وإجراءات إدارة نطاق .mz. نحن عضو في مجموعة التنمية لإفريقيا الجنوبية، وهذا جزء من مجموعة التنمية لإفريقيا الجنوبية واجتماعاتها الوزارية. ولطالما شارك فيها الوزراء المسؤولون عن تقنية المعلومات والاتصالات. هناك مؤشرات واضحة على أنه يتعين على الدول الأعضاء العمل على تنفيذ الإمتدادات الأمنية لنظام اسم النطاق في بلدانهم، ونحن في موزمبيق نفعل ذلك أيضًا. لننتقل إلى الشريحة التالية، رجاءً.

كما نتابع الجانب التنموي الوطني، على الصعيدي المحلي والدولي. أود أن أشارككم اتفاقية مالابو، واتفاقية الاتحاد الأفريقي المتعلقة بالأمن السيبراني وحماية البيانات، وكون موزامبيق هي إحدى الدول الموقعة على تلك الاتفاقية. وأننا نتابع عن كثب عمل الأمم المتحدة في إعداد اقتراح اتفاقية الأمم المتحدة لمناهضة استخدام تقنية المعلومات والاتصالات لأغراض إجرامية. ونعمل أيضًا على الانضمام إلى اتفاقية بودابست كجزء من ممارساتنا الدولية. لننتقل إلى الشريحة التالية، رجاءً.

فيما يتعلق بإجراءات الأمن السيبراني، فقد وافقت حكومة موزمبيق على السياسة والاستراتيجية الوطنية للأمن السيبراني في عام 2021، وحددت آلية التنسيق لأجل حوكمة الأمن السيبراني. وفي الهيكل الذي أعرضه هنا، يرأس تلك اللجنة الوزير الذي يشرف على تقنية المعلومات والاتصالات ولديه بالفعل دور السكرتير الفني. ومن أعضاء لجنة الأمن السيبراني هذه: وكالات إنفاذ القانون، ووزارة العدل، ومنظم تقنية المعلومات والاتصالات، والجهة التنظيمية للاتصالات، والأوساط الأكاديمية، وفرقة الاستجابة لحوادث أمن الكمبيوتر الوطنية، والمجتمع المدني، والقطاع الخاص. لذلك نتبع نهج أصحاب المصلحة المتعددين في إنشاء هذه اللجنة للإشراف على عملية تنفيذ الأمن السيبراني في الدولة. لننتقل إلى الشريحة التالية، رجاءً.

تحدد الاستراتيجية الوطنية للأمن السيبراني 25 مبادرة مقسمة على سبعة مجالات. أشارك هنا باللون الأحمر المجالات المتعلقة بهذا الموضوع الذي نغطيه اليوم، وهي المبادئ التوجيهية المطورة والأدوات القانونية والتنظيمية لحماية البنية التحتية الحيوية، وتعزيز الإطار القانوني للأمن السيبراني، وإنشاء مركز بحث وتحليل لحركة المرور على الإنترنت. إلى جانب إنشاء فرقة الاستجابة لحوادث أمن الكمبيوتر الوطنية وكذلك شبكة فرقة الاستجابة لحوادث أمن الكمبيوتر الوطنية ورسم خرائط للبنية التحتية للمعلومات الحيوية. نعتقد أن هذه الأنشطة مرتبطة بطريقة ما بنطاق المستوى الأعلى لرمز البلد والأمن السيبراني بسبب دور الإنترنت في تشغيل الأمن السيبراني للبنية التحتية الحيوية. لننتقل إلى الشريحة التالية، رجاءً.

نعتقد أن هذه الأنشطة مرتبطة بطريقة ما بنطاق المستوى الأعلى لرمز البلد والأمن السيبراني بسبب دور الإنترنت في تشغيل الأمن السيبراني للبنية التحتية الحيوية. لذلك نحن نعد قانون الأمن السيبراني وقانون حماية البيانات وكذلك قانون الجرائم الإلكترونية. ونحن في صدد العمل على لائحة التسجيل والترخيص لمزود الخدمة الوسيط ومشغلي المنصات الرقمية. وسندرج أيضًا لوائح أخرى سيتم تطويرها خلال السنوات القادمة، والتي ترتبط بعمل نطاق المستوى الأعلى لرمز البلد فيما يتعلق بالأمن السيبراني. لننتقل إلى الشريحة التالية، رجاءً.

فيما يتعلق بتطوير الإطار القانوني، نعتقد أن لدينا دورًا رئيسيًا نلعبه بصفتنا الجهة المنظمة لتقنية المعلومات والاتصالات، ونحن المسؤولون عن إعداد مقترحات القوانين لتقديمها حتى يتمكن المشروعون من متابعة العملية التشريعية، بالتالي نحن يمكننا التأثير على اللائحة والأدوات المعيارية الأخرى المتعلقة بنطاق المستوى الأعلى لرمز البلد. يمكننا اقتراح تغيير الأدوات المعيارية المتعلقة بنطاق المستوى الأعلى لرمز البلد والأمن السيبراني. وبصفتنا مدير نطاق المستوى الأعلى لرمز البلد، فإن المعهد الوطني لتقنية المعلومات والاتصالات مسؤول عن إدارة وتدبير نطاق .mz وكذلك توفير خدمات تحليل الاسم والحفاظ على البنية التحتية الحيوية اللازمة لإكمال عمل استعلامات DNS وتوفير خدمات التسجيل لأمناء التسجيل، والتي يمكن أن تشمل إنشاء أو إلغاء أسماء النطاقات وتحديث خادم الأسماء. نعتقد أيضًا أنه في هذا المجال، يلعب المعهد الوطني لتقنية المعلومات والاتصالات دورًا مهمًا في مواءمة الأدوات المعيارية للأمن السيبراني، وكذلك العمل الفني لتنفيذ آلية الأمن السيبراني المتعلقة بـ DNS أو نطاق المستوى الأعلى لرمز البلد. لننتقل إلى الشريحة التالية، رجاءً.

هذه هي الشريحة الأخيرة، ونحن نعتقد أن مراجعة سياسات تسجيل النطاق الجديدة بموجب نطاق المستوى الأعلى لرمز البلد الموزمبيقي ستتضمن جوانب أمنية. سنعمل على تنفيذ البنية التحتية لأمان نطاق المستوى الأعلى لرمز البلد مع التركيز على الإمتدادات الأمنية لنظام اسم النطاق. سنلتزم بتوصية مقدم الخدمة الوسيط بمجرد الموافقة على قانون الأمن السيبراني الجديد ولوائح تسجيل مقدمي الخدمات الوسطاء. سنعمل أيضًا على الامتثال لاتفاقية بودابست بمجرد اكتمال عملية الانضمام. سنلتزم بسياسات ICANN الخاصة بنطاق المستوى الأعلى لرمز البلد ونطاقات TLD الأخرى والجوانب الأخرى المتعلقة بإدارة الإنترنت. لننتقل إلى الشريحة التالية، رجاءً.

هذه هي الشريحة الأخيرة من عرضي التقديمي. نشكركم على اهتمامكم ونأسف لكوني سريعًا بعض الشيء بالنسبة للفريق الفني الذي يدعم الترجمة. شكراً لك.

أناليز ويليامز: شكرًا جزيلًا لك يا لورينو. أي أسئلة لـ "لورينو"؟ نعم من فضلك، يا أنيل.

أنيل جاين: شكراً لك. يعمل المعهد الوطني لتقنية المعلومات والاتصالات كجهة منظم، ويعمل أيضًا كمدير لنطاق المستوى الأعلى لرمز البلد. ألا تشعر أن هذه الأدوار متعارضة مع بعضها؟

لورينو شيمان: شكرًا لك على هذا السؤال. في الواقع، نحن لسنا المنظمين فقط لتقنية المعلومات والاتصالات. نحن نعمل أيضًا كهيئة للأمن السيبراني. نحن نعمل أيضًا بصفتنا مسئولين عن نطاق المستوى الأعلى لرمز البلد. بشكل عام، لدينا مهمة الإشراف على تطوير الإنترنت في الدولة. لذا فإن دور المنظم للخدمة الرقمية هو أحد الأدوار، لكنه ليس الدور الوحيد.

أنت تسأل هل تتعارض في المصالح أم لا. نعتقد أن هناك آليات حوكمة يتم وضعها بمشاركة جميع أصحاب المصلحة في الدولة وهي ما يساعدنا في الإشراف على الأنشطة التي يضطلع بها المعهد. نحن دولة نامية ذات قيود كبيرة من حيث الموارد المالية، ولسنا في وضع يسمح لنا بامتلاك كيانات متعددة، اعتمادًا على المجالات الجديدة المتعلقة بتطوير التقنيات الرقمية.

على سبيل المثال، لدينا حتى الآن منظمان، أحدهما الجهة المنظمة الاتصالات، والآخر المعهد الوطني لتقنية المعلومات والاتصالات، وهو منظم تقنية المعلومات والاتصالات، بما في ذلك المجالات الأخرى التي ذكرتها للتو.

أناليز ويليامز: شكرًا، لورينو. أية أسئلة أخرى؟ لا أرى أي أسئلة في الغرفة. ولا أسئلة في Zoom. لذا قد ننتقل إلى المتحدث التالي الآن. شكراً لك. إذن المتحدثة التالية هي روزاليا موراليس. إنها المديرة التنفيذية لمركز معلومات الشبكة بكوستاريكا، ونطاق المستوى الأعلى لرمز البلد .CR. شاركت روزاليا في نطاق .CR منذ عام 2012. لقد قادت مشاريع تتعلق بحوكمة الإنترنت، مثل: نقاط تبادل شبكات الإنترنت، الأمن السيبراني، البنية التحتية للإنترنت، وسياسة الإنترنت، وكانت سابقًا عضوًا في مجلس إدارة سجل عناوين الإنترنت لأمريكا اللاتينية ومنطقة الكاريبي. لقد شاركت في مجموعات عمل في منظمة دعم أسماء النطاقات لرمز البلد ومؤسسة ICANN وجمعية نطاق المستوى الأعلى لأمريكا اللاتينية ومنطقة الكاريبي ومنتدى حوكمة الإنترنت المحلي في كوستاريكا. روزاليا، من فضلك. مرحبًا بكم جميعًا. سأقدم نظرة عامة على مبادرات الأمن السيبراني وكيف أثرت تشريعات الأمن السيبراني على نطاق المستوى الأعلى لرمز البلد الخاصة بنا. لننتقل إلى الشريحة التالية، رجاءً.

أولًا، سأقدم نظرة عامة حول معنى الأمن السيبراني في نطاق المستوى الأعلى لرمز البلد الخاص بنا، ثم التشريعات بشكل عام. لننتقل إلى الشريحة التالية، رجاءً. بالنسبة لنطاق .CR، يعد الأمن السيبراني قضية رئيسية ذات أهمية. لقد عملنا في مجال الأمن السيبراني بشكل مكثف على مدار الـ 12 عامًا الماضية. وبهذا، أعني أننا جزء من فرقة الاستجابة لحوادث أمن الكمبيوتر الوطنية في كوستاريكا. نحن جزء من مجلس الإدارة. لقد عملنا مع الحكومة، مع مقدمي خدمات الإنترنت والمنظمات الأخرى، والمؤسسات الرئيسية في البنية التحتية لكوستاريكا، في توفير ورش عمل مع الوكالات المحلية والدولية. وعملنا أيضًا في مشاريع تعاون دولية مختلفة للمساعدة في البنية التحتية للأمن السيبراني في البلاد.

كما ذكرتُ، نحن جزء من فرقة الاستجابة لحوادث أمن الكمبيوتر الوطنية. نحن في الواقع المنظمة التي قدمت المعدات الأولى لفرقة الاستجابة لحوادث أمن الكمبيوتر الحكومية. لقد بدأنا بالدورات التدريبية وبالقدرات الفنية للحكومة الوطنية لبدء مبادرات الأمن السيبراني محليًا. وقمنا

بتنظيم دورات تدريبية وبرامج توعية للمدارس والجامعات والمجتمع التقني في كوستاريكا. بشكل عام، سياساتنا، كما ذكر الكثير منا في العروض التقديمية السابقة، هي أننا لسنا مسؤولين عن المحتوى. ولأي نوع من التغيير يمكننا إجراؤه على نطاق ما، سنحتاج إلى أمر محكمة لإجراء أي تغييرات على أي من نطاقاتنا كجزء من قضية أو قضية تتعلق بالأمن السيبراني محليًا أو دوليًا. لننتقل إلى الشريحة التالية، رجاءً.

حتى الآن في كوستاريكا، صدقنا على اتفاقية بودابست في عام 2017 من قبل الكونغرس المحلي لدينا. ومع ذلك، يوجد حاليًا تأخير في التشريعات التكميلية الأخرى التي تحتاج إلى تمريرها حتى تعمل هذه الاتفاقية بالفعل بشكل مناسب أو يكون لديها استجابة سريعة من وكالاتنا المحلية. من القضايا الرئيسية هي الوكيل المتخفي الافتراضي. هذا قانون يجب إنشاؤه وإقراره. في هذه المرحلة، إنها مجرد فكرة ومناقشة تجري في كوستاريكا، لكن لم يتم التصديق عليها. والثانية هي الدليل الرقمي. هناك بروتوكول لسلطاتنا المحلية يتعلق بكيفية التعامل مع الأدلة الرقمية. ولكن عندما يتعلق الأمر باتفاقية بودابست، فإنها في الواقع تفتقر إلى الطابع التشريعي الرسمي الذي تحتاجه لكي تتم العملية وفقًا لذلك وبسرعة حسب حاجة السلطات الدولية.

ثانيًا، لقد قبلنا البروتوكول الإضافي الثاني لاتفاقية بودابست في عام 2022. لم يتم التصديق عليه في الكونجرس إذ لا يزال هناك دولتان تحتاجان إلى الالتزام بهذا التعديل حتى يتم تمريره إلى مجلسنا المحلي. لذلك نحن فقط نتابع المناقشات. ومنها التأثير الذي سيحدثه هذا التعديل في نظام WHOIS، لكننا ما زلنا ننتظر أن يتم التمرير من قبل الهيئة التشريعية والتصديق عليه فعليًا. ونحن نعتمد على نظرائنا الأوروبيين المحليين للقيام بعمل رائع ومساعدتنا في ذلك.

ثانيًا، هناك قانون الجرائم الإلكترونية، وهو أول قانون تم تمريره في كوستاريكا يؤثر بشكل مباشر على كيفية إدارة قضايا الأمن السيبراني محليًا. وتم تمرير ذلك في عام 2013. ولقد ساعدنا بالفعل. ولم يؤثر على سياساتنا أو عملياتنا. لقد ساعدنا بالفعل لأنه وفر مسارًا لعملائنا المحليين حول كيفية المضي قدمًا إذا كان لديهم أي تعارض. في الماضي، كانت منطقة رمادية إلى حد كبير ولم يكن هناك الكثير مما يمكنهم فعله. والآن يوجد بالفعل مسار واضح لكيفية الوصول إلى السلطات المحلية والقيام بشيء ما بشأن جرائم الأمن السيبراني التي قد تحدث في مجالاتهم. وأخيرًا، هناك معاهدة الأمم المتحدة للجرائم الإلكترونية التي تجري مناقشتها حاليًا في الأمم المتحدة. اتخذت كوستاريكا موقفًا محايدًا للغاية. وعلى هذا النحو، نحن فقط نشاهد ونرى

ما يحدث. حتى الآن، نحن مجرد متفرجين ونأمل أن نرى ما سينتج عن تلك المناقشات. لننتقل إلى الشريحة التالية، رجاءً.

هناك مبادرات أخرى أثرت على مساحة الأمن السيبراني محليًا وكذلك كيفية عملنا كنطاق المستوى الأعلى لرمز البلد، وليس بالضرورة قانونًا تم تمريره من قبل الكونجرس، ولكنه يؤثر على عملياتنا. كما ذكرت، فإن فرقة الاستجابة لحوادث أمن الكمبيوتر الوطني هي شيء كنا جزءًا منه طوال الوقت منذ إنشائه. وحاليًا، كان في الفصل الدراسي الأخير اهتمام كبير بتقوية فرقة الاستجابة لحوادث أمن الكمبيوتر والمعدات الموجودة بها، والتدريب والموظفين. بالإضافة إلى تدريب محلي للوكالات الوطنية وجميع المنظمات الأخرى مثل نطاق .CR الذي توفر الاستقرار للإنترنت في كوستاريكا. وقد قدمت حكومة الولايات المتحدة تمويلًا كبيرًا لحكومتنا لتعزيز الأمن السيبراني. ونحن جزء من المنظمات التي تساعد الحكومة في إجراء تدريبات مكثفة في مجال الأمن السيبراني.

وهذه التدريبات لم تبدأ. ومع ذلك، فقد طُلب منا أن نكون جزءًا منها، ونحن ننتظر لنرى ما سيحدث. إنه مشروع من المفترض أن يستمر حوالي خمس سنوات. لذلك قد يقع عبء التركيز على الأمن السيبراني على كاهل الحكومة، وعادة ما يعتمد حتى الدور الذي نلعبه مع الحكومة على الحكومة المسؤولة في تلك النقطة الزمنية المحددة. الأمر غير مستقر. بعض الحكومات مشاركة في الأمر للغاية. والبعض الآخر ليس كذلك. في هذه الحالة، يكونون مشاركين جدًا. منذ العام الماضي، عانت كوستاريكا من بعض حوادث القرصنة الهامة على خزينتنا وخدمة الرعاية الصحية لدينا. لأكثر من ستة أشهر تم اختراقها وخلق أزمة وطنية. لذلك منذ ذلك الحين، ولهذا السبب تلقينا مساعدة دولية، وأصبحت نقطة مهمة للحكومة الحالية ومنظمتنا على هذا النحو.

ثم هناك أيضًا إستراتيجية للأمن السيبراني تم إنشاؤها، وتم الانتهاء منها العام الماضي في عام 2022. هذه استراتيجية وضعتها وزارة التكنولوجيا والعلوم والاتصالات بالتعاون مع منظمة البلدان الأمريكية OAS. لم تؤثر إستراتيجية الأمن السيبراني هذه علينا أو على سياساتنا أو على العمل يوميًا بشكل مباشر. لقد كنا جزءًا من المناقشات وجلسات التعليقات لهذه الاستراتيجية. بشكل عام، الأمر واسع للغاية، وهذا جهد بذلته منظمة الدول الأمريكية في بلدان مختلفة في جميع أنحاء المنطقة. لذا فهي مشابهة جدًا للاستراتيجيات الأخرى التي نفذتها منظمة الدول الأمريكية في بلدان أخرى. لذلك لا تنطبق بالضرورة بشكل مباشر على واقعنا المحدد لبلدنا. الأمر واسع

النطاق للغاية. لذلك لم يؤثر ذلك على طريقة عملنا. نحن في الواقع جزء من جلسات التعليقات، كما ذكرت.

حاليًا، هناك قانون يتم تمريره لإنشاء وكالة للأمن السيبراني. أصبحت هذه الوكالة أكثر نقاشًا وقد يكون لها تأثير على نطاق المستوى الأعلى لرمز البلد وعملياتنا، وبشكل عام، كيفية إدارة البيانات في الدولة. لم يصادق الكونغرس عليها، ولا يبدو أنها ستحظى بالموافقة في هذه المرحلة، لكن الأمر قد يتغير. المناقشات في الكونجرس تتغير بشكل كبير. على هذا النحو، يمكن للقانون أن يتغير. عادة، عند إجراء المناقشات، قد يضيفون تعديلات أو يحذفونها، ونحن فقط نراقب ونرى ما يحدث للتأكد من أنه لا يؤثر على عملياتنا بطريقة سلبية. وإذا كان هناك أي طريقة يمكننا من خلالها المساعدة فعليًا في تحسين الأمر، فسنكون بالتأكيد متاحين لتقديم ملاحظات حول هذا القانون. لأنني أعتقد أن القانون يوافق نية هذه الحكومة الجديدة لتحسين وترسيخ الموافقة على تشريعات الأمن السيبراني في كوستاريكا. ويتم دفعه بسرعة كبيرة، وأعتقد أنه لا يزال بحاجة إلى بعض النقاش. إذ لم ينته بعد. لننتقل إلى الشريحة التالية، رجاءً.

بشكل عام، الاستنتاجات هي أنه طوال 12 عامًا تقريبًا من العمل عن كثب مع مختلف منظمات الأمن السيبراني في الدولة، أنشأنا علاقة قوية مع وكالات إنفاذ القانون. وقد ساعدنا ذلك في إجراء حوار مفتوح حول السياسات والمشاريع المختلفة وأي شيء في مجال الأمن السيبراني يمكن أن يؤثر على نطاق المستوى الأعلى لرمز البلد الخاص بنا. عادة ما نجري اتصالات مكثفة مع الوكالات المعنية مما سمح لنا بمعرفة ما يجري والتأكد أيضًا من أنه يساعد كلا الطرفين أو جميع الأطراف المعنية.

علاوة على ذلك، يعد الأمن السيبراني حاليًا مجال اهتمام رئيسي لحكومتنا و نطاق المستوى الأعلى لرمز البلد بشكل عام، مما يجلب بعض المخاطر. كما ذكرتُ، هناك بعض القوانين الجارية، وبالتالي ما زلنا لا نعرف بالضرورة ما سيكون المنتج النهائي. لكننا سنراقب عن كثب للتأكد من أنه يحسن بالفعل مساحة الأمن السيبراني ولا يخلق نوعًا من الخطر أو المخاطرة للمستخدم النهائي أو نطاق المستوى الأعلى لرمز البلد.

بشكل عام، هناك الكثير من العمل في المستقبل. بدأت كوستاريكا لتوها العمل مع تشريعات الأمن السيبراني. على هذا النحو، لدينا الكثير لنتعلمه من نطاقات المستوى الأعلى لرموز البلدان الأخرى، والعديد منها في هذه اللجنة، فيما يتعلق بكيفية إدارة إنشاء هذه القوانين الجديدة وكيفية

التعلم من تجربتهم ومعرفة كيف يمكننا التأثير أو تحسين تشريعاتنا المحلية للأمن السيبراني حتى نتأكد من أن نطاقات المستوى الأعلى لرمز البلد الخاصة بنا قد تم تعزيزها بواسطة هذا المجلس التشريعي وليس بطريقة أخرى. كما توفر فرصًا للعمل مع السلطات من كوستاريكا وخارجها. لقد أتاحت لنا الفرصة حتى لتدريب موظفينا على أحدث تقنيات الأمن السيبراني، وبالتالي أصبحوا المدربين الوطنيين للوكالات الأخرى محليًا ويساعدون في نقل المعرفة والجهود المستمرة لإنشاء إنترنت أكثر استقرارًا وأمانًا في كوستاريكا. شكراً لك.

أناليز ويليامز: شكرًا جزيلًا، روزاليا. أيوجد أسئلة لـ "روزاليا"؟ أولجا، تفضلي.

أولغا كافالي: شكراً لك. شكرًا لجميع المقدمين. عروض شيقة جدًا. وأنا أشكركم جزيلاً على ذلك. وهذا سؤال لروزاليا. أعلم أنكِ قلتِ إن هذا قانون جديد تمامًا تفكر فيه في كوستاريكا. بشأن هذه الوكالة التي تفكر فيها، هل لديكِ أي فكرة عن كيفية ملاءمتها للهيكل البيروقراطي للحكومة؟ هل ستعتمد بشكل مباشر على الرئاسة أم كيف ستتفاعل مع وزارات الأمن والدفاع الأخرى؟ وربما لا تتوفر لديكِ هذه المعلومات، ولكن فقط في حالة توفرها. شكراً لك.

روزاليا موراليز: شكرا لكِ، أولغا. نعم، هذا القانون تم إنشاؤه بالفعل من قبل وزارة التقنية والعلوم والاتصالات. جزء من المشكلة مع هذا القانون هو أنه يمنح الوزارة بعض الصلاحيات التي يتمتع بها النظام القضائي بالفعل ووزارة العدل في الواقع. على سبيل المثال، أفهم أنه يوفر للوزارة القدرة على التحدث إلى الإنتربول وتبادل المعلومات، وهو أمر لا تمتلك الوزارة بالضرورة حاليًا الموظفين أو القدرة أو الخبرة للقيام به. لذلك فهو جزء من الحوار الجاري. لذلك أعتقد أنه يخلط قليلًا بين الأدوار التي يجب أن تقوم بها كل وزارة على حدة. وكان هذا جزءًا من مشكلة عدم تمرير القانون. لكنه مدفوعة من قبل وزارة العلوم والتكنولوجيا والاتصالات.

أناليز ويليامز: شكراً لك. أية أسئلة أخرى؟ لا أرى أي أسئلة في الغرفة ولا في Zoom. لذلك ربما، نظرًا لأن، دينا دقيقتين كما أعتقد، كنت سأطرح سؤالًا على روزاليا، لكنني أعتقد أنني أوجهه إلى جميع أعضاء اللجنة في النهاية. كنا نتحدث في استراحة القهوة عن مدى صعوبة الحفاظ على جميع المبادرات التشريعية الناشئة. لذلك عندما نصل إلى النهاية، قد أطلب من جميع المتحدثين فقط مساعدتنا في فهم كيف تحافظ سجلاتهم على ذلك كله. لكن في الوقت الحالي، سننتقل إلى آخر متحدث لدينا. المتحدث الأخير لدينا هو باربرا بوفسي، رئيسة نطاق المستوى الأعلى لرمز البلد بسلوفينيا ورئيسة مجلس السجلات الوطنية الأوروبية لنطاقات المستوى الأعلى. تتمتع باربرا بخبرة تزيد عن 20 عامًا في الإدارة وإدارة الأعمال وسياسة الاتحاد الأوروبي وخبرة واسعة في نظام اسم النطاق، وعمل اسم النطاق، والخصوصية وأمن المعلومات. باربرا، تفضلي.

باربرا بوفس: شكرًا لك، أناليزا. يومًا سعيدًا لكم جميعًا. شكرًا للمقدمة اللطيفة. نعم، لدي الكثير من الخبرة، كما يمكن للمرء أن يقول. حتى أنني أتذكر عندما كانت جميع المعايير المشتركة تحت رادار المشرعين. نعم، لن تصدقوا أننا لم نكن منظمين على الإطلاق. بالتأكيد، لقد مرت هذه الأوقات. لذلك من الجيد أن أكون آخر المتحدثين. قيل لي إنها مزحة أن يتم تشريع أفضل منتج للتصدير في أوروبا. لست متأكدة تمامًا هل عليّ الاعتذار أم أنكم ستتقبلون الأمر فقط.

أولًا، أود أن أشكرك، مارثا موريرا، التي ساعدتني في هذا العرض التقديمي. لذا سأتحدث عن كيفية تعامل النطاق .SI و.PT جزئيًا مع هذا الكم الهائل من التشريعات، ومعظمها في مجال الأمن السيبراني، ولكن أيضًا في بعض القطاعات الأخرى. لذا أشكر أيضًا بولينا من مجلس السجلات الوطنية الأوروبية لنطاقات المستوى الأعلى التي تحققت من أن جميع الحقائق صحيحة، لأنني لست محامية. لكن جميع الأخطاء التي قد أرتكبها، هي مني أنا. الشريحة التالية، من فضلك.

ربما تكون على دراية بأن ليس—جميع الدول الأوروبية لا تعاني من قوانينها الوطنية فحسب. لكنها كذلك بالفعل. نحن نخضع جميعًا إلى إطار قانوني أوروبي كبير. إليكم المصادر القانونية لقانون الاتحاد، وكيف يمتثلون إليه. لننتقل إلى الشريحة التالية، حيث إنني لا أنوي القيام بعرض تقديمي مفصل حول من يفعل ماذا في الاتحاد الأوروبي ومن هو المسؤول عن كل تشريع وكيف يتم اتخاذ كل هذه القرارات. ففي النهاية النتيجة هي وجود التوجيهات أو اللوائح. لكن بإمكانكم

أن تستنتجوا من هذه النقاط والأسهم أن الأمر معقد للغاية. ولابد لي من الاعتراف بأنني ما زلت غير راض عن كل الإجراءات المنتشرة.

ولحسن الحظ، أنا لست مضطرًا إلى ذلك. هذا بفضل العمل الرائع الذي نحصل عليه من مجلس السجلات الوطنية الأوروبية لنطاقات المستوى الأعلى (CENTR)، لا سيما جزء السياسة لأحد الفرق الصغيرة بالمجلس (CENTR). فمن منظور سجل صغير جدًا مثلنا، أعتقد أننا لن نكون قادرين حتى على متابعة ما يجري. ناهيكم عن أن التأثير سيكون غير محتمل. لننتقل إلى الشريحة التالية، رجاءً.

إليكم قائمة بقوانين الأمن السيبراني الخاصة بالاتحاد الأوروبي والمتعلقة برمز البلد (CC) القائمة بالفعل. كانت هذه بداية أول توجيهات أمن نظام الشبكات والمعلومات، وهي خطوة صغيرة في خضم تشريعات الأمن السيبراني واسعة النطاق المتبعة والتي تؤثر على سجلات نطاق المستوى الأعلى لرمز البلد (ccTLD). إذ أصبحنا مؤهلين في ذلك الوقت للعمل كمزودي الخدمات الأساسية. يختلف الأمر قليلًا عن الخدمات الهامة، ولكن أجل، لدينا الكثير من المسؤوليات الجديدة. الآن، لدينا التوجيهات المنقحة حول أمن الشبكات وأنظمة المعلومات (NIS 2) مع بعض المتطلبات الإضافية. نحن الآن بصدد ترجمة التوجيهات المنقحة حول أمن الشبكات وأنظمة المعلومات (NIS 2) إلى ووفق التشريعات الوطنية. نظرًا لترجمة توجيهات أمن نظام الشبكات والمعلومات (NIS 1) بطريقة مختلفة تمامًا باختلاف البلدان، يسعى المشرعون الآن إلى تنسيق ذلك. فقط كي أوضح لكم مدى تأثير ذلك على أعمالنا. في معظم الأحيان نتحدث عن المادة (21) بشأن التحقق من المسجل، وما زال هناك الكثير من الأمور غير الواضحة. ومن ثم، لدينا التزامات الإبلاغ. هناك أيضًا بعض الإرشادات الصادرة عن وكالة الاتحاد الأوروبي للأمن السيبراني (ENISA). ها هي الإجراءات الأمنية لمشغلي نطاق المستوى الأعلى (TLD)، ولكن هناك إجراءً جديدًا يتعلق بالتحقق من المسجل. هذه الإجراءات غير ملزمة، لكنها ما زالت توصيات. الشريحة التالية، من فضلك.

لم يُنجز هذا الجزء حتى الآن. ما زال هناك بعض التشريعات في مجال الأمن السيبراني قيد الإعداد، ولكنها ليست جاهزة تمامًا في الاتحاد الأوروبي. يوجد تغييرات يومية. لكن كما ذكرت من قبل، لحسن الحظ نتلقى تقاريرًا شاملة من العاملين بمجلس السجلات الوطنية الأوروبية

لنطاقات المستوى الأعلى (CENTR) والتي تنطوي أيضًا على أهمية نطاقات المستوى الأعلى لرمز البلدان (ccTLD). وهذه نقطة هامة للغاية. لننتقل إلى الشريحة التالية، رجاءً.

كيف لنا أن نتعامل مع كل هذه المبادرات؟ نسعى مع مجلس السجلات الوطنية الأوروبية لنطاقات المستوى الأعلى (CENTR) ومجموعة التنسيق، ولدينا مجموعة عمل قانونية وتنظيمية حيث ننسق ونطلع على ما يجري. لذلك، نحاول التأثير على التشريعات القادمة عند الانتهاء من إعدادها على مستوى الاتحاد الأوروبي. نحن لا ننتظر سن التشريع، ولكن عندما تكون هناك مسودة أولى، نحاول التأثير في المجالات التي يواجهنا فيها. نقوم بذلك باستخدام أوراق البحثية الخاصة بمجلس السجلات الوطنية الأوروبية لنطاقات المستوى الأعلى (CENTR) والتي يمكنكم الاطلاع عليها على صفحة مجلس السجلات الوطنية الأوروبية لنطاقات المستوى الأعلى (CENTR)، إلى جانب عقد العديد من الاجتماعات على مستوى الاتحاد الأوروبي مع المشرعين حيث إننا نحاول التأثير في جميع مراحل العملية.

ومن ثم بصفتنا أعضاء فرادى، نحاول إبلاغ أعضاء البرلمان الأوروبي الوطنيين بحيث يكونوا على علم بوجود تشريعات جديدة قيد الإعداد وماهيتها، على سبيل المثال، من خلال توصياتنا ببعض التعديلات. ورد أيضًا أن مجلس السجلات الوطنية الأوروبية لنطاقات المستوى الأعلى (CENTR) أسس مؤخرًا مراكز تحليل ومشاركة المعلومات (ISAC) لنطاقات المستوى الأعلى (TLD). وهذه من الأشياء الهامة بالنسبة للأمن السيبراني. كذلك هناك الكثير من التوعية والمشاركة والتدريب على مستوى الاتحاد الأوروبي. الشريحة التالية من فضلك.

ماذا عن المستوى الوطني لدينا؟ الرسالة الرئيسية تتلخص في إنني أعتقد أنه ينبغي أن يكون نطاق المستوى الأعلى لرمز البلد (ccTLD) استباقيًا بقدر الإمكان إذا أردنا التأثير على العملية. كما ذكرت من قبل، نحن نحاول التأثير على العملية على مستوى الاتحاد الأوروبي من خلال الممثلين الوطنيين، ومن ثم يصل الأمر إلى اعتماد التشريعات الوطنية. نحاول التحدث إلى جميع المستويات وإلى الجمهور والوزارات وجميع المشرعين، ونحاول تثقيفهم لأنهم بحاجة إلى فهم الأساسيات والمعنى الحقيقي لبعض الإجراءات على مستوى نظام اسم النطاق (DNS). أعتقد أننا تمكنا من ذلك على مدار السنوات، ربما كان الأمر أسهل في سلوفينيا. فهي دولة صغيرة ولطيفة للغاية، ويُقدر عدد سكانها بنحو بمليوني شخص. بعد خطوتين فقط ستجد الشخص المناسب للتحدث معه. كما أنها تساعدنا في كوننا مشغلًا تقنيًا، حيث نشارك بصورة أكبر في مجال

السياسة. لذلك، نسعى إلى جلب خبراء تقنيين وغير تقنيين على الصعيد الوطني في محاولة منا لجعلهم يتحدثون بنفس اللغة. لننتقل إلى الشريحة التالية، رجاءً.

يمكنني أنا أذكر هنا القنوات التي نستخدمها بجميع أنواعها. لذلك، نشارك في مناقشات عامة. نلجأ إلى جهات الاتصال لدى الوزارات. نكتب بعض المقالات والمدونات. نرسل رسائل البريد الإلكتروني. نتصل هاتفيًا بالأشخاص. وبالطبع، عندما يكون هناك تشريع وتُجرى عملية المشاورات العامة، إن لم يكن قبل ذلك، نحاول التأثير في ذلك الوقت. في بعض الأحيان، تمكنا من حصد النجاح، وفي البعض الآخر بالكاد تمكنا من تحقيقه. ربما يتعلق الأمر بتنفيذ لوائح شبكة التعاون لحماية المستهلك (CPC). وهي اللوائح التنظيمية لحماية المستهلك عبر الحدود. حققنا هنا نجاحًا باهرًا، وتواصلنا بشكل جيد للغاية مع الوزارة المسؤولة عن التنفيذ، وحصلنا على نتائج معقولة.

لم نحصل على نتائج جيدة حيال تنفيذ التوجيهات المنقحة حول أمن الشبكات وأنظمة المعلومات (NIS2). تقوم الجهة التنظيمية الوطنية الآن بعملها ولا ترغب في التحدث إلى أي شخص. ونتمنى أن يتغير هذا الأمر في القريب. أعتقد أنه لأمر غاية في الأهمية أن نتحدث مع بعضنا البعض، لأننا بصفتنا CC نهتم كثيرًا بالإنترنت الآمن تمامًا كحكومتنا. نحن بحاجة فقط إلى التأكد من أن اللوائح أو التشريعات التي نحصل عليها قابلة للتطبيق، وأنه يمكننا القيام بما هو مطلوب، وأن هذا هو الإجراء الصحيح الذي يتعين إنجازه. في بعض الأحيان لا يوجد ما يكفي من الفهم لذلك. لننتقل إلى الشريحة التالية، رجاءً.

إذن كيف يؤثر هذا على أعمالنا؟ نعم، نحاول التفكير في المستقبل، لذلك لا ننتظر اعتماد التشريعات. نحاول الاستعداد مسبقًا، بالطبع، نحن نتحسن في التنبؤ بالمستقبل. لذلك، نتابع العملية منذ البداية بمساعدة مجلس السجلات الوطنية الأوروبية لنطاقات المستوى الأعلى (CENTR) في كثير من الأحيان. ولأن مجلس السجلات الوطنية الأوروبية لنطاقات المستوى الأعلى (CENTR) هو مجتمع عظيم، فقد تعلمنا أيضًا من بعضنا البعض كثيرًا ونساعد بعضنا البعض ونتشارك الموارد، وهذا حقًا - خاصة بالنسبة لسجل صغير مثلنا - أمر في غاية الأهمية.

ما فعلناه، حتى قبل توجيهات أمن نظام الشبكات والمعلومات (NIS)، قررنا الحصول على شهادة ISO 27001، واتضح أن هذا القرار كان صائبًا للغاية، لأنه لم يكن هناك الكثير من العمل مع توجيهات أمن نظام الشبكات والمعلومات في بادئ الأمر. لا يزال لدينا بعض العمل للقيام

بإجراءات التحقق من التسجيل. ونحن نعمل على ذلك. نعم، الامتثال هو الموضوع الساخن في أوروبا. في جميع المجالات، على الرغم من صعوبة تحقيق هذا الأمر، فإننا نعمل على ذلك.

إذن ما قصدته بتأثير بروكسل هو أن بروكسل هي القوة الرائدة في تشريعات الأمن السيبراني، وأعتقد أنه لأمر مهم أن نضع التشريعات، لكننا لسنا بمفردنا. لذا فإن المتطلبات الجديدة تضع الكثير من القوة وتتطلبها أيضًا. نعم، حصلنا على الكثير من الالتزامات الجديدة التي تجعل التسجيل يتكبد بعض التكاليف. نحن بحاجة إلى تغيير إجراءاتنا. نحن بحاجة إلى العثور على أشخاص جديدة يمكنها التعامل مع الإجراءات الجديدة. نحن بحاجة إلى القيام باستثمارات مالية كبيرة في البنية التحتية لدينا. لذلك، أصبح الأمر أكثر صعوبة. كذلك مع وجود هذه المتطلبات الجديدة، أصبحت إجراءات تسجيل نطاق المستوى الأعلى لرمز البلد (ccTLD) أكثر تعقيدًا بالنسبة للمسجل النهائي. فهل هذا يعني أنهم سئموا من ذلك وسيذهبون إلى مكان يسهل فيه الحصول على اسم نطاق؟ هذا بإمكانه أن يخلق مشكلة فى البقاء، إلى جانب التنافس مع رموز البلدان (CC) الأخرى وكذلك نطاقات المستوى الأعلى العامة (gTLD). ولكن من ناحية أخرى، أعتقد أننا جميعًا نريد إعادة بناء الثقة في الإنترنت. لذا في النهاية، أعتقد أننا سنحقق توازنًا مثاليًا بين إثقال الكاهل والراحة التامة. بالطبع، سنواصل العمل معًا لأننا عبارة عن مجموعة من السجلات تتقاسم نفس العبء سواء كثُر أو قل. على الأقل يمكننا أن نشتكي إلى بعضنا البعض. لكن كلا، فإننا نتبادل الموارد وهذا مجدي حقًا. أعتقد أنني انتهيت. هل هذه الشريحة الأخيرة؟

أناليز ويليامز: نعم. شكرًا لك، باربارا. أعتقد أن النقطة التي أشرت إليها حول التفكير المستقبلي والاستباقية وعدم انتظار حدوث الأشياء من حولك مهمة للغاية. هل هناك أية أسئلة موجهة إلى "باربارا"، رجاءً؟

أوجو أكيري: شكراً لك. اسمي "أوجو أكيري". لقد كنت جزءًا من .ng. سؤالي لباربرا هو، عندما تقول إن بعض الدول الأوروبية تخلفت عن الركب، فهل هذا يعني أن سياسة مثل القانون العام لحماية البيانات يُجرى اعتمادها الآن في جميع أنحاء الاتحاد من قبل جميع أعضاء الاتحاد الأوروبي؟

باربرا بوفس: شكرًا على سؤالك. لا، لقد أسأت الفهم. كلا، هذا لا يعني أن بعض الدول الأوروبية قد تخلفت عن الركب. ربما أخطأت. كما قلت، كافة الأخطاء ترجع لي بالكامل. لا، لقد كنت أقصد التشريعات. أعني أن الإطار القانوني هو الإطار نفسه تمامًا بالنسبة لك وللأعضاء الأوروبيين. لذلك هذا ما عنيته بنفسه بالنسبة لنا جميعًا. ما فكرت به أو ما قصدت قوله هو أن هناك الكثير من العبء الملقى على عاتق نطاقات المستوى الأعلى لرمز البلدان (ccTLD) الأوروبية. هكذا كنت أقصد نطاقات المستوى الأعلى لرمز البلدان (ccTLD) الأوروبية ربما يتم الضغط عليها أكثر من غيرها. هذا ما كنت أقصده.

أناليز ويليامز: شكرًا لك، باربارا. أعتقد أن لدينا سؤالاً هنا ويوجد سؤال آخر في غرفة Zoom، لكننا سنذهب إلى الغرفى أولًا. مرحبًا بكم.

عمر كونتريراس: معكم "عمر كونتريراس". أعمل لدى شركة Identity Digital Inc. من ضمن الأشياء التي نالت إعجابي واستحساني من بداية العرض التقديمي إلى نهايته كان التعاون. لقد أخذتِ في الاعتبار أن لدينا موارد محدودة وأننا نعمل بوضوح مع البرتغال ومجلس السجلات الوطنية الأوروبية لنطاقات المستوى الأعلى (CENTR) لتحقيق أقصى استفادة من الإمكانات التي لدينا. أتساءل عما إذا كان لديكِ أية توصيات بشأن نطاقات المستوى الأعلى لرمز البلدان (ccTLD) خارج أوروبا للحصول على هذا النوع من التعاون، والتفكير في أمريكا الوسطى، ولاسيما أمريكا الجنوبية؟ كيف بدأتِ تلك القنوات؟ كيف تمكنتِ من فرز هذه المجالات والعثور عليها على الأقل لتطوير نوع من الموارد معًا في محاولة لمواكبة ذلك ببساطة؟ هل لديك نصائح أو حيل أو اقتراحات ترغبين في مشاركتها؟

باربرا بوفس: شكرًا. بلى، من المحتمل أن يكون الوضع مختلفًا في أوروبا لأننا نتشارك نفس الإطار القانوني. وهذا ما يُسهل الأمر—على الرغم من أن التنفيذ على الصعيد الوطني يمكن أن يواجه بعض الاختلافات، فضلًا عن وجود بعض القوانين الوطنية المختلفة لدينا. ومع ذلك، هناك إطار عمل

نعمل جميعًا في ظله. لكنني أعتقد أنه عندما كنت أستمع إلى كل هذه العروض التقديمية، كان الأمر نفسه في كوستاريكا أو فانواتو. إلى حد ما هو نفس التشريع المعمول به بشكل أو بآخر. لذلك أعتقد أن المنظمة الإقليمية المعنية مثل أوروبا هي مجلس السجلات الوطنية الأوروبية لنطاقات المستوى الأعلى (CENTR) ويمكن لجميع المنظمات الأخرى أن تفسح المجال بعض الشيء للمحامين أو الأشخاص السياسيين للالتقاء ومناقشة كيف يمكنهم إيجاد أرضية مشتركة.

أناليز ويليامز: شكرًا لك، باربارا. سنتلقى الآن سؤالاً من غرفة Zoom. نعم، ميشيل، تفضل.

ميشيل نيلون: أنا موجود بالفعل بشكل شخصي في الغرفة. شكراً لك. صباح الخير. ميشيل نيلون أعمل لدى شركة Blacknight للسجل ولكل هذه الأمور. باربرا، من ناحية العبء التنظيمي، أعني من الواضح أنكِ تنظرين إليه بشكل خاص من منظور السجل. أود أن أنظر إليه أكثر من منظور المسجل مع محاولة تسديد الفواتير وكسب المال من هذا المجال. هل لديكِ أي فكرة عما إذا كانت المفوضية الأوروبية وأصدقاؤها لديهم أي فهم للوضع التنافسي غير المؤات الذي يضعوننا فيه جميعًا في ظل هذه الأعباء التنظيمية؟ لأنه - أعني - عندما أنظر كيف يضحك الأمريكيون علينا من الناحية العملية في كل مرة يرون فيها ظهور مثل هذه الأشياء الجديدة، أعني إنه لأمر محبط للغاية. لمجرد المعرفة، هل هناك أي ضوء في نهاية النفق أم أننا سنظل غارقين في الأعمال الورقية؟

باربرا بوفس: أعتذر بشدة. لا أعتقد أن لدي أخبارًا جيدة في هذا الصدد، لكن هذا ما أردت قوله. حسنًا، لقد ذكرت السجلات فقط ولم يكن ذلك منصفًا. هذا صحيح. الجميع - وليس فقط السجلات - وكذلك المسجلون والشركات بشكل عام تواجه هذه المشكلات، مع الحفاظ على القدرة التنافسية في هذا المجال شديد التنظيم. ولا أعتقد أنني حصلت على إجابة. وأنا أتفق معك في ذلك إذا كان ذلك سيساعد.

ميشيل نيلون: انظري، أنا أقبل بأي شيئ. أشعر بالسعادة عندما يتفق معي أي سجل.

أناليز ويليامز: شكرًا. هل هناك أي أسئلة أخرى موجهة إلى "باربارا"؟ أرى بروس.

بروس تونكين: شكرًا لك، أناليزا. أتساءل عن مستوى الصورة الأشمل، لأنه يبدو على مر التاريخ أن كل رموز البلدان (CC) داخل أوروبا توصلت بشكل مستقل إلى قواعد هذا النوع من العمل في مجتمعها. لكنكِ الآن تتحدثين على المستوى الإقليمي. وعندما ألقي نظرة على الكثير من هذه التغييرات، هل هي مدفوعة بتغييرات أوسع في مجالات أخرى من الاقتصاد مع أضرار جانبية؟ بعبارة أخرى، بُنيت عناصر البنية التحتية الأمنية والحيوية للتعامل مع القطاعات الصناعية الرئيسية. كما لو أنه حسنًا سنضيف أسماء النطاقات إلى ذلك أيضًا. أو هناك قلق بشأن الخصوصية أو تساؤلات بشأن قواعد اعرف عميلك. بعبارة أخرى، هل يرون بالفعل مشكلة في صناعة أسماء النطاقات نفسها؟ أم أنهم يحلون مشكلة أكبر ومن ثم نجد أنفسنا متورطين في هذه المعضلة؟

باربرا بوفس: أتسألني هل هم يحاولون حلها؟ هل تقصد المفوضية الأوروبية أم ماذا؟

بروس تونكين: نعم، أعني المفوضية الأوروبية. بمعنى آخر، ما المشكلة التي يحاولون حلها؟

باربرا بوفس: أعتقد حقًا أنهم يحاولون - لكن هذا مجرد تخمين.

لا أدري. لكن الهدف الرئيسي هو إعادة بناء الثقة في الإنترنت. وأن هذا هو الهدف الرئيسي. وكيف تقومون بذلك؟ لا أدري.

بروس تونكين: إذن هذا يبدو وكأنه اقتصاد رقمي على نطاق أوسع، أليس كذلك؟ لذا فهم يحاولون بناء الثقة في الاقتصاد الرقمي الذي نحن جزء منه. هل ذلك صحيح؟ أنا أطرح السؤال.

باربرا بوفس: الآن، فقدتني.

بروس تونكين: أنا أحاول فقط أن أفهم ما هو الدافع الأساسي وراء كل هذه اللاوئح في صناعة أسماء النطاقات في أوروبا؟

باربرا بوفس: لست متأكدًا تمامًا - ربما لست الشخص المناسب لأسأله.

بارت بوسوينكل: أناليز، أنا بارت. قد يكون هذا سؤالًا مثيرًا للاهتمام للغاية بالنسبة للجنة منسقي علاقات حوكمة الإنترنت للغوص فيه.

أناليز ويليامز: لدينا العديد من الأعضاء من منطقة الاتحاد الأوروبي، لذا يمكننا إضافة ذلك إلى القائمة أيضًا. شكرًا بارت. لقد لمحتُ سؤالًا هنا. لدينا كريس، وأنا أرى يد جوردان في غرفة Zoom. تفضل يا كريس.

كريس ديسبين: شكرًا لك، أناليز. لدي بضعة نقاط أود مناقشتها. لذا للإجابة على سؤال ميشيل أو على الأقل إبداء رأيي حول إجابة سؤال ميشيل، أعتقد في الواقع أنهم لا يهتمون. أعتقد أنهم مصممون فقط على

التشريع لما لم يحققوه من خلال نموذج أصحاب المصلحة المتعددين. وحقيقة أنه يتم استهدافه في نطاقات المستوى الأعلى لرمز البلد بشكل رئيسي هو لأنه ليس لديهم خيار، لأنهم إذا كانوا سيحاولون ويفعلون أمرًا ما، فسيضطرون للتشريع فقط لنطاقات المستوى الأعلى لرمز البلد. على الرغم من أنك إذا تحدثت إلى بعض المنظمين الأوروبيين، فسوف يخبرونك أنه حسبما يعرفون، فإنه ينطبق على الجميع. وهذا لا يحدث، لكنهم سيخبرونك أنه يحدث.

وفقط لأهمية الأمر، أجريت جلسة العام الماضي في المدرسة الصيفية الأوروبية للحديث عن التفتيت.

وكان أحد أعضاء اللجنة، ولن أسميهم لأن هذا غير لائق، أحد كبار المسؤولين في المفوضية الأوروبية هو الذي قال، نعم، نحن نقوم بتفتيت الإنترنت لأنك لن تفعل ما نريد. هذه هي الخلفية.

أناليز ويليامز: شكرًا يا كريس. أعتقد أن هذا تعليقك، لكنني سأذهب إلى جوردن بعد ذلك.

جوردان كارتر: شكرًا. أعدك أن هذا سؤال، يا جوردان كارتر. باربرا، هل تعتقدين أن الطريقة التي يقوم بها الاتحاد الأوروبي بالتنظيم بهذه الوتيرة العالية تتوافق مع دعمه العام لنموذج أصحاب المصلحة المتعددين؟

باربرا بوفس: لقد أصبت مربط الفرس.

أناليز ويليامز: ولكن ربما يكون هذا أمرًا آخر يمكننا تناوله كمناقشة جماعية. كما اقترح بارت، يمكننا أن نضيف هذا إلى مناقشة اللجنة ككل، بدلاً من وضعه على الفور للحصول على وجهات نظر شخصية، باربرا. هل هناك أي أسئلة أخيرة لباربرا أو لأي من المتحدثين الآخرين اليوم؟ ميشيل.

ميشيل نيلون: أريد فقط أن أعبر عن شكري لكم ولمجلس السجلات الوطنية الأوروبية لنطاقات المستوى الأعلى لأنكم كنتم مفيدين جدًا جدًا خلال العام الماضي في مساعدتنا جميعًا لمحاولة الخروج من الجنون، الذي يخرج من المفوضية الأوروبية. أعني، من الطبيعي أن يكون هناك ما يؤخرنا وما يساعدنا بالطبع. الحقيقة هي أن المفوضية الأوروبية تحاول تنظيم الأمور لأنني أعتقد، كما قال كريس، أنهم لا خيار لديهم. لذا فهم يدفعونها ليتم تمريرها ولا يأبهون بالأمر. ومحاولة التبحر في الأمر هي صراع شاق. أنا أعلم أننا جميعًا سنمضي الكثير من الوقت في القلق بشأن التوجيهات المنقحة حول أمن الشبكات وأنظمة المعلومات وبعض هذه الأشياء الأخرى خلال الفترة القادمة. ويحتاج بقيتكم ممن هم خارج الاتحاد الأوروبي إلى إبقاء أعينهم مفتوحة لأن حكوماتكم ستبدأ على الأرجح بالقول، أوه، انظروا إلى ما فعله الأوروبيون. على صعيد آخر، يضحك الأمريكيون على طول الطريق. لكن شكرًا. لقد كان مجلس السجلات الوطنية الأوروبية لنطاقات المستوى الأعلى مفيدًا جدًا. إنه حقًا موضع تقدير.

باربرا بوفس: شكرًا جزيلًا. إذا كان السجل سعيدًا، فأنا سعيد.

أناليز ويليامز: حسنًا، بشأن هذه الملاحظة، أعتقد أننا انتهينا.أعتقد أننا سمعنا من جميع المتحدثين لدينا اليوم أن الأمن السيبراني هو مجال رئيسي للقلق بالنسبة لجميع الحكومات.

هناك الكثير من التشريعات المعمول بها بالفعل والمزيد قيد التنفيذ. لذلك من الرائع أن تتاح هذه الفرصة للاستماع إلى بعضنا البعض والتعلم من بعضنا البعض. وأرجو أن تشكروا جميع المتحدثين اليوم. وأردت أن أعبر عن تقديري لنورمان ولورينو، اللذين قدما للتو عروضهما التقديمية الأولى في مؤسسة ccNSO. شكراً لك.

[نهاية التدوين النصي]