ICANN68 | منتدى السياسات الافتراضي - الجلسة العامة: نظام اسم النطاق وإنترنت الأشياء: الفرص والمخاطر والتحديات
الثلاثاء 23 حزيران (يونيو) 2020 – من الساعة 01:00 م إلى 02:30 بتوقيت ماليزيا

ريا أوتانيس: مرحباً، وأهلًا بكم في الجلسة العامة بشأن نظام اسم النطاق DNS وإنترنت الأشياء: الفرص والمخاطر والتحديات. اسمي ريا أوتانيس، وأنا مديرة المشاركة عن بعد لهذه الجلسة.

يرجى ملاحظة أن هذه الجلسة قيد التسجيل وتتبع معايير السلوك المتوقعة من ICANN. خلال هذه الجلسة، لن يُسمح بقراءة الأسئلة أو التعليقات إلا إذا تم تقديمها باللغة الإنجليزية داخل خانة الأسئلة والأجوبة. يمكن الوصول إلى هذه الميزة من شريط الأدوات على برنامج زووم Zoom. سأقرأ الأسئلة والتعليقات المسموح بها خلال الوقت الذي حدده رئيس الجلسة أو مسير الجلسة. إذا كنت ترغب في طرح سؤالك أو إبداء تعليقك شفهيًا، فيرجى رفع يدك. عند الاستدعاء، سيتم منحك الإذن بإعادة صوت الميكروفون. يُرجى إلغاء كتم صوت الميكروفون في هذا الوقت والتحدث. اذكر اسمك للسجل واللغة التي ستتحدثها إذا كنت تتحدث بلغة غير الإنجليزية. تتضمن هذه الجلسة التدوين النصي والترجمة الفورية في الوقت الفعلي. لعرض النسخ في الوقت الحقيقي، انقر فوق زر التسمية التوضيحية المغلقة في شريط أدوات برنامج زووم Zoom.

لمساعدة المترجمين الفوريين، يرجى التكلم بوضوح وبسرعة معقولة. لسماع الترجمة الفورية، ستحتاج إلى تنزيل تطبيق الترجمة الفورية. يمكن العثور على مزيد من المعلومات في تفاصيل الجلسة على جدول الاجتماع، والتعليمات موجودة في الدردشة.

أخيرًا، أود أن أذكرك باستخدام القائمة المنسدلة في لوحة الدردشة للتبديل من الرد على جميع أعضاء اللجنة، للرد على أعضاء اللجنة والحضور إذا كنت ترغب في أن يقرأ الجميع في الغرفة تعليقات الدردشة.

بهذا، سأسلم الكلمة إلى أليخاندرا رينوسو. أليخاندرا، تفضلي رجاءً.

أليخاندرا رينوسو: شكرًا جزيلاً لك، ريا.

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

مع أطيب التمنيات للجميع. أُدعى أليخاندرا رينوسو. أعمل لدى grant Thornton، نطاق ccTLD في غواتيمالا ويشرفني أن أترأس هذه الجلسة العامة.

يعد إنترنت الأشياء بجعل حياتنا أسهل وأن تكون مجتمعاتنا أكثر أمانًا وذكاءً واستدامة من خلال عشرات المليارات من الأجهزة المتصلة التي تتأثر بشكل سلبي ومستقل وتعمل على بيئتنا المادية. في حين أن هذا يجعل إنترنت الأشياء مختلفًا تمامًا عن تطبيقات الإنترنت التفاعلية التقليدية مثل البريد الإلكتروني وتصفح الويب، فإن العديد من أجهزة إنترنت الأشياء ستستخدم نظام اسم النطاق لتحديد الخدمات عن بُعد التي تحتاجها.

نشرت اللجنة الاستشارية للأمان والاستقرار، SSAC، مؤخرًا الوثيقة SAC105، وهو تقرير يناقش فرص ومخاطر وتحديات التفاعل بين DNS وإنترنت الأشياء. ستعطي الجلسة العامة لهذا اليوم المزيد من الجوهر للحوار الذي تهدف هذه الوثيقة إلى إطلاقه، وتحديداً من خلال تمكين أفراد المجتمع من جميع الدوائر من مناقشة الموضوع مع الخبراء المتخصصين وكذلك مع بعضهم البعض.

هذه الجلسة العامة هي متابعة من جلسة ccNSO حول SAC105 في اجتماع مونتريال والتي ركزت بشكل خاص على ccTLDs.

تهدف هذه الجلسة العامة إلى فهم أفضل لكيفية اختلاف إنترنت الأشياء عن تطبيقات الإنترنت التفاعلية التقليدية وكيفية استخدام DNS؛ لفهم أفضل لكيفية تفكير مشغلي DNS وإنترنت الأشياء في التفاعل بين المنظومتين من حيث الفرص والمخاطر والتحديات؛ وتعزيز التفكير في الدور الذي يمكن أن يلعبه مجتمع ICANN في هذا الفضاء.

الشريحة التالية من فضلك.

سيكون هذا جدول أعمال اليوم. أولاً، ستكون هناك لمحة موجزة عن الوثيقة SAC105. ثم سيكون لدينا لجنة خبراء لتبادل وجهات نظرهم حول الموضوع. بعد ذلك، سيكون هناك مراجعة من النظراء حيث سيقدم المراجعون ملاحظات حول العروض التقديمية من الخبراء. وسوف ننتهي بأسئلة وأجوبة من الجمهور.

الشريحة التالية من فضلك.

اسمحوا لي أن أقدم لكم بإيجاز كريستيان هيسلمان الذي سيقدم لنا لمحة عامة عن SAC105.

كريستيان هو مدير SIDN Labs، وهو الفريق البحثي لـ SIDN، مشغل نطاق المستوى الأعلى لرمز البلد NL. في هولندا. وهدفها هو تعزيز الأمن التشغيلي والمرونة لاتصالات الإنترنت من طرف إلى طرف من خلال البحث التجريبي القائم على القياس التجريبي ووضع نماذج وتقييم أنظمة وأدوات الإنترنت الجديدة.

كريستيان أيضًا عضو في SSAC وقيادة فريق عمل SSAC الذي أنتج SAC105 ونظام DNS وإنترنت الأشياء والفرص والمخاطر والتحديات.

وهو أيضًا أستاذ مشارك بدوام جزئي في جامعة تفينتي بهولندا، ويرأس مجلس الإدارة في NLNetLabs.

كريستيان، الكلمة لك.

كريستيان هاسلمان: حسنًا. شكرًا جزيلاً لك، أليخاندرا.

لذا يشرفني اليوم أن أقدم لكم لمحة عامة قصيرة عن SAC105، وهو التقرير الذي أصدرته SSAC في حزيران (يونيو) من عام 2019. وكما لخصت أليخاندرا بالفعل، فإن هذه الوثيقة تدور حول التفاعل بين إنترنت الأشياء IoT ونظام DNS مع التركيز بشكل خاص على إثارة وتسهيل المناقشة في مجتمع ICANN.

لذلك سيظهر هذا التقرير أيضًا كورقة تمت مراجعتها من قبل النظراء في مجلة تسمى IEEE Internet Computing في وقت لاحق من هذا العام.

الشريحة التالية من فضلك.

إذن إنترنت الأشياء. ما استخدمناه كتعريف في تقريرنا هو تعريف إنترنت الأشياء الذي أعطته ISOC في عام 2015 وهو تطبيق - حسنًا، ما يقوله هناك، يوسع اتصال الشبكة وقدرات الحوسبة إلى الأشياء والأجهزة وأجهزة الاستشعار والعناصر التي لا تعتبر عادة أجهزة كمبيوتر. لذا القيام بتوصيل كل شيء بالشبكة بشكل أساسي لم تكن تفكر في الاتصال به من قبل.

الاختلافات مع التطبيقات التفاعلية التقليدية، كما تعلمون، مثل البريد الإلكتروني وتصفح الويب، وبعضها ما يلي. لذا فإن إنترنت الأشياء يستشعر ويتفاعل باستمرار مع الفضاء المادي. هذا فرق مهم. كما أنه يفسر المعلومات التي يتلقاها من أجهزة استشعار مختلفة للعمل فعليًا على هذا الفضاء. يحدث هذا عادةً دون وعي المستخدم، لذا فكر في أجهزة استشعار صغيرة مضمنة، كما تعلمون، في الجدران وأنواع أخرى من الأشياء التي تتفاعل معها دون معرفتها حقًا. هذا ما يسميه الأشخاص من ISOC بالتفاعل السلبي على عكس التفاعل التفاعلي الذي قد تحصل عليه مع متصفحات الويب وعملاء البريد الإلكتروني، على سبيل المثال. لذلك ستكون هناك كمية هائلة من أجهزة إنترنت الأشياء هذه. على الأقل هذا هو توقع العديد من محللي السوق. لذا، فإن الأشخاص يذكرون أعدادًا من 20 إلى 30 مليارًا من هذه الأجهزة، وهم، كما تعلمون، يعملون بشكل أساسي في خلفية حياتنا اليومية. لذلك نحن لا نراهم في الواقع. نتفاعل معهم دون أن ندركهم.

كما أن الفرق هو أن أجهزة إنترنت الأشياء عادة ما تكون غير متجانسة أكثر بكثير مما اعتدنا عليه من حيث أجهزة الكمبيوتر المحمولة والهواتف المحمولة. لذلك نحن نتحدث عن أنواع مختلفة من أنظمة التشغيل. نحن نتحدث عن بنى الأجهزة المختلفة، ونتحدث أيضًا عن أنواع مختلفة من اتصالات الشبكة. لذا فهو ليس مجرد واي فاي. إنه أيضًا ZigBee، وهو أيضًا أنواع أخرى من الشبكات اللاسلكية.

حسنًا. وأخيرًا أيضًا، يختلف إنترنت الأشياء في أن أجهزة إنترنت الأشياء لها عمر أطول بكثير، ربما لأنها مدمجة في الهياكل المادية، على سبيل المثال، وتتميز أيضًا بتشغيلها غير المراقب. لذلك لا يوجد مدير شبكة أو أي شيء من هذا القبيل يهتم حقًا بهذه الأجهزة. إنهم فقط يجلسون هناك ويفعلون ما يفعلونه ويتصلون بالشبكة دون أن تعرفوا ذلك.

لذا تعتبر إنترنت الأشياء هي الشيء الكبير التالي، كما تعلمون، لبعض الوقت الآن. في الواقع، هذه الأشياء مستمرة منذ التسعينيات، وأعتقد أنها كانت تسمى الحوسبة المنتشرة أو شيء من هذا القبيل. لذلك كانت هناك أسماء مختلفة تقريبًا لنفس المفهوم. ولكن على أي حال، نحن الآن في مرحلة حيث من الممكن نشر هذه الأنواع من الأجهزة وأجهزة الاستشعار والمشغلات، ونتيجة لذلك، يعتقد الناس أن هناك - اعتقادًا قويًا بأن إنترنت الأشياء سوف توفر مجتمعًا أكثر أمنًا وذكاء وأكثر استدامة. على سبيل المثال، في مجال أنظمة النقل الذكية، توجيه ندفق البيانات بذكاء عبر منطقة حضرية، على سبيل المثال، بناءً على جميع أنواع أجهزة

الاستشعار، أو شبكات الطاقة الذكية أو ربما المنازل الذكية والمدن الذكية. أعتقد أن هذا الأخير هو المثال الأكثر جاذبية لأن هذا ما نعرفه جميعًا بسبب كل الأشياء التي لدينا في منازلنا في هذا اليوم وهذا العصر.

حسنًا. إذن هناك الكثير من الأمل في إنترنت الأشياء، كما تعلمون، ولكن هناك مشكلة رئيسية واحدة، وهي أمن إنترنت الأشياء، وسأتحدث عن ذلك في غضون دقيقة.

الشريحة التالية من فضلك.

شكرًا.

إذن هذا مثال على - هذا هو النموذج الذي نستخدمه في - SSAC للتفكير في إنترنت الأشياء. إذن ما تراه هنا هو نوع من الصورة المزدحمة للمساحات المادية على اليسار، لذا فلنأخذ الجزء العلوي. إذاً، ما تراه في أعلى اليسار هم أشخاص في منازلهم، ويتفاعلون مع ما نسميه نشر إنترنت الأشياء. هذه في الأساس المنطقة المظللة كما تراها في منتصف الشاشة. ويتكون نشر إنترنت الأشياء من ثلاثة أشياء مختلفة. واحد هو أجهزة إنترنت الأشياء. اثنان هو اتصال الشبكة. وثلاثة خدمات خلفية، أليس كذلك؟

لذلك هناك مثال هنا مع ساعة صغيرة وقفل باب ذكي حيث عندما يقترب شخص ما من الباب ويقترب الناس من باب منزلهم وربما يكون لديهم أيضًا نوع من مقبض الباب الذكي، يتم جمع كل هذه المعلومات حول القرب من قبل - ساعة ذكية يرتديها الأشخاص بالاشتراك مع، كما تعلمون، بصمات الأصابع التي يتم إجراؤها بواسطة مقبض الباب الذكي، ويتم إرسال المعلومات عبر الإنترنت إلى خدمة في مكان ما خدمة بعيدة، وبناءً على تلك الخدمة، يتم اتخاذ القرار، حسنًا، دعونا نفتح قفل الباب أم لا. وذلك حتى يكون مدفوعًا بسياسة المستخدم، من الواضح.

إذن ما ترونه هو أنه في هذا المثال البسيط، هناك معلومات يتم استشعارها بواسطة الجهاز العلوي، D1، بواسطة الساعة الذكية، على سبيل المثال. تتم مشاركة هذه المعلومات عبر الإنترنت إلى خدمة ما ثم يتم إرسالها مرة أخرى إلى قفل الباب لقفله أو إلغاء قفله.

إذن ما تراه هو الاستشعار والعمل الجسدي - استشعار البيئة المادية للمستخدم والتعامل معها، ويتم ذلك بشفافية - دون أن يكون المستخدمون على علم بها، أليس كذلك؟

لذلك يرى المستخدمون الأجهزة فقط، حيث يرون ساعاتهم الذكية ويرون مقبض الباب الذكي، على سبيل المثال، لكنهم لا يرون آلية كاملة تقف وراء ذلك.

وأحد الأجزاء في تلك الآلية هو نظام اسم النطاق، لأن ما نعرفه من بحث سابق هو أن هذه الأجهزة لديها - إنها تتفاعل مع الخدمات على الإنترنت لتقديم وظائفها، أليس كذلك؟ لذلك - وهذا يختلف عن تصفح الويب التقليدي حيث تتفاعل مع متصفح الويب لالتقاط بعض المعلومات من الويب أو لاستخدام الخدمة. هذا - في هذه الكوكبة، تستخدم الأجهزة خدمات لأداء وظيفتها، أليس كذلك؟

على سبيل المثال، في هذه الحالة المحددة، يمكن أن تحلل الخدمة معلومات المستشعر الواردة من المستخدم ثم تتخذ قرارًا بشأن فتح قفل الباب أم لا. حسنًا؟

لذا في هذه التفاعلات، يلعب DNS دورًا مهمًا، لكنني لن أناقش التفاصيل لأن إليوت سيتحدث عن ذلك أكثر بعد هذا العرض التقديمي.

حسنًا. أعتقد أن هذا هو الجزء الأكثر أهمية في الوقت الحالي، لذا يرجى المتابعة إلى الشريحة التالية.

حسنًا. إذن هذا التقرير يسمى DNS وفرص إنترنت الأشياء والمخاطر والتحديات. لذلك لدي شريحة في كل من هذه الثلاثة: واحدة للفرص، واحدة للمخاطر، وواحدة للتحديات. والفرص هي شيء لا نتحدث عنه عادةً في DNS لأنه - في SSAC لأننا نركز في الغالب على التهديدات والمخاطر، كما ينبغي، ولكن في هذه الحالة اعتقدنا أن هناك حاجة - كانت هناك فرصة لـ DNS لأنها عالمية - كما تعلمون، إنها بنية تحتية للثقة العالمية، يمكنك القول، يمكنها أن تزيد من خصوصية وأمان وشفافية إنترنت الأشياء. لذا نعتقد حقًا أن DNS يمكن أن يوفر قيمة مضافة هنا.

لذلك أدرجت ثلاثة هنا. مزيد من التفاصيل في SAC105. إذن الأول هو أننا نعتقد أن نظام اسم النطاق يمكن أن يقلل من خطر تصنيف المستخدمين، وذلك لأن هذه الأجهزة التي تحدثنا عنها للتو، تتفاعل مع نظام اسم النطاق. لذا، فإن استعلامات نظام اسم النطاق، إذا كان هناك مراقب بين مسار جهاز إنترنت الأشياء والخدمة البعيدة التي يستخدمها، فيمكنه أن يرى، بناءً على تفاعلات نظام اسم النطاق، ما يستخدم الشخص في منزله، على سبيل المثال، نوع الأجهزة

التي يستخدم أو ماذا - ربما حتى لو كانوا يستخدمون جهازًا، لأن ذلك يخلق المزيد من التفاعلات مع DNS.

والاحتمال الآخر هو أنه إذا كنت تعرف أي أجهزة إنترنت الأشياء التي يتم استخدامها من خلال النظر في أسماء النطاقات، يمكنك حتى - كمهاجم، يمكنك حتى محاولة الظهور - في محاولة لمعرفة ما هو جهاز إنترنت الأشياء الذي يولد هذه الاستفسارات، أليس كذلك؟ لذلك هناك المزيد من الأبحاث التي تظهر أن العديد من أجهزة إنترنت الأشياء تستخدم مجموعة صغيرة من أسماء النطاقات التي يبحثون عنها، لذلك للعثور على الخدمة عن بعد التي تحدثنا عنها للتو في شريحة سابقة. وأحيانًا استعلامات DNS هذه أو أسماء النطاقات التي يستخدمونها، تكشف أيضًا عن معلومات حول نوع الجهاز الذي ينشئها، حسنًا؟ إذن هذا هو التفكير وراء هذا الجزء من تقليل مخاطر ملفات تعريف المستخدمين. ويمكنك تحقيق ذلك من خلال تشفير طلبات DNS التي تولدها أجهزة إنترنت الأشياء هذه. لذلك يمكنك القيام بذلك، على سبيل المثال، من خلال DoH و/أو DoT والتي هي محل جدل كبير.

فرصة أخرى نتوقعها هي للتخفيف من المخاطر حيث يتم إعادة توجيه أجهزة إنترنت الأشياء إلى خدمة بعيدة أخرى. لذا، على سبيل المثال، رأينا - على الإنترنت، رأينا مفهومًا يسمى اختطاف التوجيه، على سبيل المثال. وتؤدي إلى إرسال تدفق البيانات إلى شبكة ضارة. وهذا شيء يمكن أن يكون له آثار شديدة في إنترنت الأشياء لأن أجهزة إنترنت الأشياء لن تتصل بعد الآن - الخدمات التي من المفترض أن تتصل بها ولكن ربما تتصل بخدمة ضارة. ويكمن الخطر في أن الأشخاص يشاركون بياناتهم مع - بيانات حميمة مع خدمات عن بعد أو يعني أن الخدمات البعيدة يمكن أن تعمل حتى على بيئتها المادية، أليس كذلك؟ وبالتالي هذا خطر.

نعتقد أن DNS يمكن أن يساعد هنا لأنه من الواضح أن لدينا DNS - DNSSEC، أليس كذلك؟ لذا يمكنها التحقق من سلامة الرسائل الصادرة من DNS. وإذا حدث اختطاف توجيه، كمثال، فسيكون عملاء DNSSEC قادرين على اكتشاف ذلك لأنهم يستطيعون - يلاحظون ذلك لأن التوقيع على رسائل DNSSEC ليس صالحًا.

وهناك فرصة أخرى هنا نراها هي أنها فرصة لأمناء السجلات لتقديم مصادقة متعددة العوامل. هذا ما يعنيه MFA.

على سبيل المثال، يمكنهم حماية أسماء النطاقات التي تستخدمها أجهزة إنترنت الأشياء بشكل أكبر باستخدام عوامل متعددة، وربما حتى التعرف على بصمات الأصابع أو شيء من هذا القبيل. حسنًا؟ هذه هي الفرصتان اللتان نراهما لتقليل مخاطر إعادة توجيه أجهزة إنترنت الأشياء من خلال خدمة ضارة.

وأخيرًا، نرى فرصة لتوفير مزيد من المعلومات حول الخدمات والحلول التي تستخدمها أجهزة إنترنت الأشياء. لذا، يتفاعل الأشخاص في معظم الأوقات مع أجهزة إنترنت الأشياء، لكنهم لا يعرفون حقًا نوع المعلومات التي يشاركونها مع الخدمات على الإنترنت. ودعونا نقول، إن جعل استعلامات DNS التي تنشئها أجهزة المستخدمين، وجعلها مرئية للمستخدمين النهائيين سيساعدهم على إعطاء المزيد من التبصر لتلك التفاعلات، حسنًا؟

لذا في المثال السابق، سترى ذلك - ستتمكن من رؤية أن ساعتك تشارك المعلومات مع خدمة عن بعد على الإنترنت، على سبيل المثال. حسنًا؟

الشريحة التالية من فضلك.

إذن هذا هو الجانب الآخر، المخاطر. لذلك ربما يجب أن أتحدث فقط عن - سأحاول جعل هذا موجزًا قليلاً. لذا فإن أكبر خطر نراه هو أن نتائج إنترنت الأشياء تؤدي إلى هجمات DDOS كبيرة على DNS، أليس كذلك؟ لذلك عندما رأينا هذا من قبل، بالطبع، المثال السيئ هو هجمات DDOS التي وقعت في عام 2016 على مشغل DNS شركة Dyn. لكننا رأينا أيضًا شبكات الروبوت الخاصة بإنترنت الأشياء تتطور على الإنترنت، ويمكن أن تنمو في الحجم بسرعة كبيرة. من المحتمل أن يبدأوا أيضًا في استخدام محللات مفتوحة من شأنها أن تعكس تدفق بيانات DDOS بعيدًا عن هدفهم، والتي قد تخلق حتى كمية أكبر من تدفق البيانات لهؤلاء الأشخاص.

والمخاطر الأخرى هي ما نسميه برمجة DNS غير ودية، والتي تستخدم DNS بطريقة ساذجة، أنه - على سبيل المثال، لدينا - قبل بضع سنوات كان هناك مثال حيث أدى تطبيق iPhone إلى إنشاء عشوائي لاستعلامات DNS والتي تسببت في تفكيك ذاكرة التخزين المؤقت الخاصة بالمحللات لأنها لم تتمكن من تخزين أي شيء مؤقتًا ونفدت سعة النسخ المتطابق الخاصة بهم.

الشريحة التالية من فضلك.

لقد رأينا - ناقشنا نموذج إنترنت الأشياء الذي قمنا بتطويره في SSAC. ناقشنا الفرص، وناقشنا المخاطر. والسؤال التالي هو: ما الذي يجب علينا فعله لاغتنام تلك التحديات ومعالجة المخاطر؟

لذلك توصلنا إلى بعض التحديات لصناعات DNS وإنترنت الأشياء التي كتبناها هنا. لذا فإن هذا يتجاوز في الواقع نطاق SSAC لأننا نعتقد أيضًا أن هناك دورًا لمجتمع إنترنت الأشياء هنا.

لذا، يتمثل الأول في تطوير مكتبة أمان لأجهزة إنترنت الأشياء هذه التي ستوفر هذه الوظائف التي تحدثنا عنها للتو في شريحة الفرص. لذلك سيكون ذلك التحقق من DNSSEC، على سبيل المثال، ودعم DoH/DoT، وكذلك الوظائف التي تجعل استعلامات DNS مرئية للمستخدمين النهائيين بطريقة جذابة وبديهية.

ثم نعتقد أن هناك تحد للتدريب. لذا، فإن تدريب خبراء إنترنت الأشياء على فهم موضوع DNS وما هي وظائفه الأمنية وما عليك القيام به لاستخدامها والعكس صحيح لخبراء DNS لفهم كيفية عمل إنترنت الأشياء بشكل أساسي وربما أيضًا إنترنت الأشياء ستغير الطريقة التي يتم بها استخدام النطاقات وربما يتطلب ذلك أنواعًا مختلفة من الوظائف لإنترنت الأشياء - لتسجيلات أسماء النطاقات والأمن.

ربما يكون البعض الآخر أكثر تحديًا، وأكثر صعوبة. لذا سيكون الأول هو التعاون مع مجموعة من مشغلي DNS لمشاركة ما نسميه بصمات DDOS. لذا ستكون هذه ملخصات لهجمات DDOS التي حدثت على مشغلي DNS هؤلاء. ثم سيتبادلون تلك المعلومات مع بعضهم البعض للاستعداد بشكل أفضل.

يمكن أن يكون أيضًا أن مشغلي DNS هؤلاء يحاولون حتى مشاركة قدرة التخفيف لـ DNS. لذا، مثل مرافق التنظيف، على سبيل المثال. ونتوقع دورًا للأنظمة في حواف الشبكة لحماية الحواف من هجمات DDOS وأيضًا ضد التطفل. التطفل على الجهاز، وهذا هو.

وأخيرًا، لنحلم قليلاً، سيكون من اللطيف جدًا، كما نعتقد، أن يكون لدينا نظام قادر على قياس تطور إنترنت الأشياء ونرى كيف ينمو وكيف يستخدم DNS.

وكانت تلك الشرائح الخاصة بي، أليخاندرا.

أليخاندرا رينوسو: شكرًا جزيلاً لك، كريستيان.

سنواصل الآن مع لجنة الخبراء لدينا الذين سيتبادلون وجهات نظرهم حول هذه المسألة بالترتيب التالي. الأول، إليوت، ليز الثانية، والثالث كريستيان.

اسمحوا لي أولاً أن أقدم لكم إليوت لير وليز فور. يعمل إليوت لير كمهندس رئيسي لشركة Cisco Systems في مجال أمن إنترنت الأشياء، مع التركيز على كيفية تواصل الجهاز والشبكة مع بعضهما البعض. لقد شارك إليوت، المخضرم في مجتمع الإنترنت، مع مجتمع IETF منذ عام 1998، وكتب عددًا من طلبات RFC، وعمل في مجلس هندسة الإنترنت، وكان قائدًا في مساهمة IETF في إعادة هيكلة ICANN أثناء انتقال الإشراف على وظائف IANA. وقد شغل أيضًا مناصب قيادية في الاتحاد الدولي للاتصالات. إليوت يقيم في سويسرا.

ليز فير هي المدير العام لجمعية مشغلي شبكات الاتصالات الأوروبية، ETNO، منذ كانون الثاني (يناير) 2016. في ETNO، تقود وتشرف على جميع الأنشطة حيث أنها الممثل الخارجي الرئيسي للجمعية.

نيابةً عن الجمعية، هي أيضًا عضو مجلس إدارة وعضو لجنة إدارية في منظمة الأمن السيبراني الأوروبية. كما تم إعادة تعيين ليز في مجلس إدارة المصلحة العامة لجمعية الإنترنت لمدة ثلاث سنوات اعتبارًا من أيار (مايو) 2019.

تتمتع ليز بخبرة تزيد عن 20 عامًا في صناعة الاتصالات. بدأت مسيرتها المهنية في وزارة العلوم والتكنولوجيا والابتكار الدنماركية حيث كتبت ونفذت التنظيم لأسواق الاتصالات. بعد ذلك، عملت في مجال الاتصالات والمشغلين والشبكات الهاتفية حيث قادت فرقًا مختلفة تتعامل مع المشكلات أثناء معالجتها لأجهزة الاتصال البيني والأجهزة المحمولة - عذرًا، خدمات الهاتف المحمول والتعاون الصناعي.

إليوت، الكلمة لك.

إليوت لير: شكرًا جزيلاً لك، أليخاندرا.

إذن الشريحة التالية، رجاءً.

أود أن أخبركم قصة فرن. هذا فرن. إنه مزود بإنترنت. تم تمكين إنترنت الأشياء. وقد اشترى ابن عمي أحد هذه الأجهزة، وقام بتثبيته، وبعد ذلك بوقت قصير قام بإنذارها في الساعة 5:30 صباحًا لإعلامها بضرورة تنظيفه. الآن، أنا شخصياً أعتبر هذا بمثابة حرمان من الخدمة. ولكن هذه هي الطريقة التي تم تصميمها للعمل.

ما لم يعرفه ابن عمي هو أنه لكي يعمل كل ذلك، كان هناك الكثير من المكونات المتوفرة في هذا الجهاز. ليس فقط أن الفرن يحتوي على عنصر تسخين وترموستات، وعزل مناسب، وجميع الأشياء الأخرى الموجودة في الأفران، ولكنه يحتوي أيضًا على جهاز إرسال/استقبال ووحدة معالجة مركزية وبعض الذاكرة وبعض المفاتيح المرنة وشاشة عرض.

هذا يمثل تهديدًا. وهذا يعني أنه يمكن مهاجمة أي شيء بهذه المكونات. إذن ما الذي يمكن القيام به في مثل هذا الهجوم؟ حسنًا، إذا كان أحدهم ناجحًا، فيمكن للمرء أن يحرق بطتي، أو في أسوأ الحالات، يمكن أن يخلق هجومًا منسقًا يتم فيه تشغيل جميع الأفران في وقت غير مناسب. لنفترض، في منطقة ليس لديها طاقة زائدة بسبب الطقس الحار وتكييف الهواء. وجميع الأفران التي تعمل في نفس الوقت تحدث انقطاع التيار.

علاوة على ذلك، يتم استخدام الكثير من مجموعة البرامج في هذا الفرن من قبل الأجهزة الأخرى، ربما مكيفات الهواء، وربما المواقد، وربما أجهزة الراديو، وربما أجراس الباب. وبالتالي يمكن تمكين الكثير من الأجهزة دفعة واحدة لتوليد طلب كبير على الطاقة. لذلك هناك حاجة إلى بعض الحماية لهذا الفرن.

الشريحة التالية من فضلك.

الشريحة التالية من فضلك.

لكي يعمل هذا الفرن - لم ينبهني مباشرة. هنا لدينا صورة للإنترنت، صورة رائعة جدًا للإنترنت تم إنشاؤها بواسطة كي سي وفريقها منذ بعض الوقت.

الشريحة التالية من فضلك.

تحدث الفرن بالفعل إلى الأجهزة الموجودة في السحابة من أجل القيام بذلك. وقد فعل ذلك كما يفعل جرس الباب. لذلك هذا هو نمط الاستخدام الشائع.

لنعد لأعلى بشريحة واحدة، من فضلك. شكرًا.

وكانت الأجهزة السحابية هي التي تواصلت بالفعل مع هاتف iPhone الخاص بها. وهذا نمط مشترك.

لكي تتمكن هذه الأجهزة من الاتصال بالسحابة، تحتاج إلى استخدام نظام اسم النطاق. لديهم نقطة نهاية سحابية. إنه شيء مثل cloud.example.com. وهذه هي الطريقة التي يتواصلون بها.

الآن، لكي يتمكنوا من التواصل في جميع المراحل على الإنترنت، يجب توجيه المعلومات بواسطة أقرب جهاز توجيه.

بالنسبة للفرن المعني، ولجرس الباب هذا، نتحدث عن الواي فاي WiFi. ولكن هناك العديد من الوسائل الأخرى للقيام بذلك. لكن الكثير من هذا يتم توصيله بالفعل من خلال المنزل، من خلال جهاز التوجيه المنزلي.

الشريحة التالية من فضلك.

فكيف يعمل هذا؟ على سبيل المثال، تتلقى استفسارًا يتعلق بالفرن - الشريحة التالية، من فضلك - حيث تقول الاستعلامات ovencloud.example.com، ويتم إرجاع عنوان IP. وعنوان IP هو شيء يأتي من عنوان محدد. الآن، ضع في اعتبارك ما قاله كريستيان. هناك حوالي 20 مليار من هذه الأجهزة الموجودة. لدينا عدد كبير من الأجهزة على الإنترنت، ولكن الفرن يحتاج فقط إلى التحدث إلى نقطة النهاية السحابية، ربما مقبض نقاط النهاية، ربما بعض الأجهزة في المنزل، لكنه لا يحتاج إلى التحدث مع كل شيء.

وهكذا إذا كان ذلك - يمكن لجهاز التوجيه المنزلي توفير نقطة تحكم، وتحد نقطة التحكم هذه من سطح التهديد في ذلك الفرن. وهذا يعني أنه حتى إذا كان هناك خلل أو ضعف في الفرن، فإن نقطة التحكم يمكن أن تحميه من هجوم واسع النطاق. هل هذا يعني أن الشركة المصنعة للفرن لا يجب أن تقدم تحديثات البرامج عندما تجد الأخطاء؟ من الواضح أن الإجابة لا. لا يزال - لا يزال هناك سطح تهديد حتى مع بعض عمليات حماية الشبكة هذه، لكن الشبكة تساعد على تقليل هذا التهديد.

الشريحة التالية من فضلك.

إذن هذا هو الاتصال الذي يذهب إلى الجهاز، نقطة النهاية السحابية التي تم حلها بواسطة DNS. لكي تعمل نقطة التحكم، يجب أن تتلقى الاستعلام والاستجابة من الفرن. هذا يعني أنه إذا كان استعلام DNS مشفرًا ولم تكن نقطة التحكم على دراية به، فلن يتمكن من توفير الحماية ولا يمكنه تقليل سطح التهديد.

الشريحة التالية من فضلك. وبالطبع يتكرر هذا مع أجراس الباب وعدد كبير من الأجهزة الاستهلاكية الأخرى.

في العالم الصناعي، تبدو الأشياء مختلفة قليلاً. اليوم أنا أركز بشكل أساسي على ما قد تراه في الأجهزة الاستهلاكية. نرى العديد من نقاط النهاية السحابية المختلفة التي تستخدمها عدة أجهزة مختلفة.

الشريحة التالية من فضلك.

فماذا يعني كل هذا؟ هذا يعني أننا بحاجة إلى - لا بأس بالتشفير. هناك سبب وجيه لتشفير استعلامات DNS، وذكر كريستيان الكثير منها. ومع ذلك، إذا كانت نقطة التحكم - إذا كان جهاز التوجيه الشبكي الذي يهدف إلى تقليل سطح التهديد لا يمكنه الوصول إلى الاستعلام نفسه، إذا لم يكن طرفًا مصرحًا به بطريقة ما لمشاهدة الاتصالات من حيث - كل من الاستعلام والاستجابة، فإن هذا الموجه لا يمكنه توفير الحماية اللازمة. لذلك هناك هذا الربط بين DNS وجهاز التوجيه الذي يتيح هذه الحماية. وقد تم توحيد هذا العمل في IETF كوسيلة لتوفير تلك الحماية.

لذلك نحن لا نقول لا تشفر. بل على العكس تمامًا. نقول شفروا. ولكن تأكد من أنه عندما تقوم بالتشفير، فإنه يتعلق بمكون مفوض بتوفير بعض (غير مسموع).

أعتقد أن هذه هي الشريحة الأخيرة.

أليخاندرا؟

أليخاندرا رينوسو: شكرًا لك، إليوت.

الآن ستكون لدينا ليز.

ليز فير: شكرًا. ومرحبًا بالجميع. سأجلب منظورًا آخر، حيث أنني قادم من جانب شركة الاتصالات، مزود خدمة الإنترنت ISP.

الشريحة التالية من فضلك.

إذا كان - سيكون العرض التقديمي الخاص بي حول لماذا من المثير للاهتمام التحدث عن 5G وإنترنت الأشياء. سأتحدث قليلاً عما يجلبه الجيل الخامس من الفرص الجديدة، ولكن أود أيضًا أن أتناول بعض المخاوف التي أثيرت حول 5G ونظام DNS، وأقول أيضًا إلى أين نرى العالم ينتقل من هنا فيما يتعلق بنظام 5G و إنترنت الأشياء ونظام DNS.

الشريحة التالية من فضلك.

لذا إذا أردنا أن نرى - تتحدث عن إنترنت الأشياء، فلماذا هذا مثير للاهتمام بالنسبة إلى 5G؟ هذا لأننا نرى بالفعل، مثل شركات الاتصالات، أن 5G، وهي مزيج من كل من الشبكات الثابتة وشبكات الجوال، إنها ليست مجرد تقنية 4G جديدة. إنها تقنية متقاربة أكثر بكثير. لذلك نرى أن ذلك سيمكن في الواقع أن يكون مكونًا مهمًا في نمو إنترنت الأشياء.

لذا ترى الأرقام هنا، والتي لا تعمل إلا على أجهزة إنترنت الأشياء المحمولة وربما تكون عددًا منخفضًا جدًا، قائلة أنه في عام 2018، رأينا 140 مليون اتصال جوال - إنترنت الأشياء، ونتوقع ما يقرب من 740 مليونًا بحلول عام 2026.

ما هو الشيء الجديد الذي سيكون مثيرًا للاهتمام في 5G؟ هل سيكون هذا هو إنترنت الأشياء المحظور الضيق، وأيضًا سيكون هناك بعض الأجهزة - بعض تحسينات MTC هي التالية - والتي ستكون تطويرًا لما هو موجود في 4G.

لذلك عندما ننظر إلى 5G، فإنه - سيكون هناك عدد من الخدمات التي تعتمد بالفعل على ما هو موجود في 2G و3G و4G، والتي تدعم بالفعل إنترنت الأشياء. ولكن سيكون إنترنت الأشياء الجديد عبارة عن المزيد من البنية التحتية IP، ومن ثم المزيد من البنية التحتية DNS.

حتى الآن، ما نراه ليس ما نسميه إنترنت الأشياء، وهو موجود على IP بقدر ما هو أكثر على الخدمات الأخرى. ونتوقع أن يكون لدينا استخدام آخر لـ 5G IoT غير الاستخدام الذي نستخدمه اليوم. ونعتقد أنه سيكون استخدامًا أفضل وأكثر أمانًا.

لذا إذا نظرنا إليها كما هو موضح في هذه الشريحة، فإن إنترنت الأشياء وأنترنت الأشياء في 5G لا ينموان في فراغ. إنها في الواقع تعتمد على مجموعة خدمات أوسع. وسيكون DNS وIP بشكل عام متحد هنا.

الشريحة التالية من فضلك.

وإذا نظرنا إلى ميراث 5G mobile ونظام DNS، فلن تكون 5G مستقلة من اليوم الأول. الآن، ما نراه هو أن هناك الكثير من شبكات 5G التي تبني على البنية التحتية 4G. إذن ما نراه هو 4G مع معدات 5G، لكنها ليست شبكة 5G كاملة.

وهناك، استخدام أسماء النطاقات وأسماء النطاقات في هذه الأنظمة الأساسية للجوّال، فهي ليست سائدة، ولكننا نستخدم الكثير من DNS، لكنها محدودة حتى الآن.

ونرى بالطبع استثناءات للتوجيه بالاعتماد على DNS حيث تعد VoLTE إحدى الحالات. ولكن ما الذي نستخدمه لاسم النطاق في نظام الهاتف المحمول؟ نرى أن اسم النطاق محدود الآن، وهي مشتقة من معرفات قديمة، والوصول إلى الإنترنت عبر الهاتف النقال غير محدد. حسنًا، هذا على الهاتف الجوّال.

لذلك لا يوجد شيء جديد في استخدام 4G إلى 5G فيما يتعلق بـ DNS، لكننا نستخدمه بنفس الطريقة في 5G كما فعلنا في 4G. الشريحة التالية من فضلك.

فلماذا 5G مثير للاهتمام ولماذا هو أكثر إثارة للاهتمام من 4G؟ هذا لأنه، كما قلت، إنها شبكة متقاربة أكثر بكثير. إنها شبكة افتراضية ستستخدم الكثير من البرامج وليس الأجهزة المعتمدة على 4G. ستكون شبكة أكثر مرونة. وكما نقول، من المفترض أن تكون أصلية IP. وعلى الرغم من صعوبة إدارة وتشغيل عناوين IPv6 لأنها طويلة جدًا، إلا أننا ما زلنا نرى استخدامًا قويًا لنظام DNS لهذا بسبب بنية IPv6.

نرى أيضًا أن نطاقنا الداخلي سيكون أصليًا لعنوان البروتوكول، وسننتقل تدريجيًا إلى IP في أسماء النطاقات بالطريقة التي ندير بها الشبكة.

إذن، في أوروبا، ما زلنا نشغل الاتصال البيني إلى حد كبير على أساس تبديل الدائرة، ولكننا نعتقد أنه مع 5G سيكون لدينا اتصال IP أكثر بكثير. هذه هي الطريقة التي يسير بها التطور في كيفية تشغيل شبكة 5G.

الشريحة التالية من فضلك.

لذلك إذا أردنا أن ننظر في كيفية تجسيد استخدام اسم النطاق، فهو في الأساس شفاف للمستخدمين بمعنى أنه غير مرئي للمستخدمين كيف نستخدم DNS. لذا فإن الطريقة التي نعمل بها مع شبكاتنا هي في الغالب للأغراض التقنية، وسيتم تضمينها في الجهاز، لذلك لا يفترض أن ترتبط باستخدام اسم النطاق. إذن الاسم ليس جزءًا مهمًا جدًا من هذا، ولكن بالطبع تقنية DNS مهمة.

ومرة أخرى، على إنترنت الأشياء، كيف يتم تنفيذه - هو المفتاح هنا حقًا، لأن الطريقة التي ننفذ بها هي التي تحدد في الواقع كيفية الإعداد. لذا، بينما نرى أن 5G ليس كذلك - لا نعتقد أن 5G سيكون مصدرًا هامًا للتسجيلات الجديدة من المستوى الثاني، نعتقد في الواقع أن هذا سيتم تحديده من خلال المزيد من النطاقات الفرعية. لذلك لا نتوقع ارتفاعًا كبيرًا في كيفية استخدامنا لأسماء النطاقات لأنه تم تعريفه على أنه نطاق فرعي أكثر استخدامًا. ومرة أخرى، لا يتم حل الكثير من هذا على الإنترنت حقًا ولكن سيتم حله كنطاق داخلي أو اسم نطاق داخلي.

الشريحة التالية من فضلك.

فلماذا نعتقد أن 5G مفيد لإنترنت الأشياء وإنترنت - ونظام DNS؟ أولاً وقبل كل شيء، نعتقد أنه على مستوى الشبكة الأساسية، سيكون لدينا، كما قلت، المزيد من البرامج وهذا سيجعل العمل مع الاتصالات من نوع الآلات في النطاق الضيق أكثر مرونة وسهولة. نحن قادرون على تحديد الشبكات بطريقة أسهل بكثير مع 5G. وعلى الجانب الأمني، سيكون تقطيع الشبكة أمرًا بالغ الأهمية بالنسبة لنا. تشريح الشبكة سيكون جزءًا من الشبكة حيث يمكننا تعريفه لهذا النوع المحدد من الاستخدام. على سبيل المثال، ستحتاج السيارات المؤتمتة، وهي إنترنت الأشياء الضخمة، إلى نطاقات منخفضة من الكمون. ولذا من المهم أن يكون لدينا نوع واحد من الخدمات للسيارات الآلية.

بالإضافة إلى ذلك، فإن استخدام الذكاء الاصطناعي الذي نعتقد أنه سيفتح بالفعل معايير شبكاتنا، سواء بالطريقة التي تجعلها أفضل ولكن أيضًا يمكننا من اكتشاف ما إذا كانت هناك أي تهديدات أو مشكلات مع الشبكات. نعتقد أن الذكاء الاصطناعي سيمكننا من العمل بشكل أسرع والعثور على المشكلات بطريقة أفضل.

لذا عد إلى التحديات، والشريحة التالية، من فضلك.

إذا نظرنا إلى ما نراه على أنه تحديات وكيف يمكننا تخفيفها، نعتقد أن تقطيع الشبكة جيد للغاية. كانت هناك مخاوف من أن هذا سيؤدي إلى تجزئة الإنترنت. نحن لا نرى هذا على أنه أي مشاكل على الإطلاق. نعتقد أن هذا سيكون مثل الشبكات الافتراضية الخاصة، ولا يزال - إنها خدمات أكثر استهدافًا للمستخدمين النهائيين ولن تخلق أي تجزئة للإنترنت.

إذا نظرنا إلى أسماء النطاقات وتجنب الاصطدام، فنحن نستخدم النطاقات العامة ولا نرى ذلك كمشكلة. إذا كان هناك أي نطاق نستخدمه للتوجيه الداخلي، فسيكون نطاقًا عامًا ولن يتم إنشاء أي تصادمات هنا.

من جانب DNSSEC، وهو أمر مهم، ستكون فرصة. إنه ليس معيارًا - إنه ليس معيارًا إلزاميًا في الوقت الحالي على 5G. لم نر أشياء من شأنها أن تخلق حاجة لامتلاك DNSSEC كمعيار في شبكة 5G، ولكن يجب استخدامه.

وبعد ذلك، مرة أخرى، عند الحرمان من الخدمات وهجمات DDOS والروبوتات، في شبكة 5G، يمكننا بالطبع معالجة ذلك. ولكن هناك اتجاه التشفير. وإذا كنت تريد مراقبة هذه الهجمات، فنحن بحاجة إلى أن نكون قادرين على رؤية تدفق البيانات.

لذلك عند الحرمان من الخدمات، إذا أردنا أن نكون جزءًا نشطًا في هذا الدفاع، فنحن بحاجة إلى أن نكون قادرين على رؤية تدفق البيانات.

الشريحة التالية من فضلك.

إذن أين ننتقل من هنا؟ لا يزال هناك العديد من الأسئلة المفتوحة حول توحيد معايير 5G. نحن فقط في صنع شبكات 5G. وكما قلت، لم نر العديد من شبكات 5G المستقلة حتى الآن. إذن ما نبني عليه الآن هو 4G مع مكونات 5G.

البنية التحتية باهظة الثمن. لذا، كما أراها، فإن 5G ليست قائمة بذاتها. 5G ليس قاب قوسين أو أدنى لأن الحالة التجارية (غير مسوع) لهذه الشبكات مكلفة للغاية.

شيء أخير هو أننا رأينا بالفعل أزمة COVID، والتي كانت أزمة مروعة بالنسبة لنا جميعًا، لكننا رأينا في جميع أنحاء العالم أن هناك تركيزًا قويًا على الحاجة إلى الرقمنة. رأينا تركيزًا أقوى على الأمن.

لذلك من هذا المنظور، رأينا أن هناك وعيًا متزايدًا بأهمية البنية التحتية، وأن الأمن مهم، وأيضًا أننا رأينا استخدامًا محسنًا لشبكاتنا. لذا نعتقد أن المستقبل سيجلب سفرًا أقل. نحن هنا اليوم. مثال جيد جدًا على عدم سفر أي منا إلى اجتماع ICANN، بدلاً من ذلك نقوم بذلك عن بُعد.

وفيما يتعلق بإنترنت الأشياء، نعتقد أيضًا أن هذا سيؤدي بالطبع، أيضًا، كنتيجة لهذه الأزمة إلى خلق المزيد من المراقبة عن بُعد والمزيد من إنترنت الأشياء.

هذا هو الجزء الخاص بي. شكرًا.

أليخاندرا رينوسو: شكرًا جزيلاً لك، ليز.

الآن سيكون لدينا كريستيان.

كريستيان هاسلمان: نعم. شكرًا لك، أليخاندرا.

لذلك أنا أبدل صفتي بشكل أساسي. سبق لي - كنت أتحدث بصفتي من SSAC. الآن أنتقل إلى صفتي كممثل لنطاق .NL، وهي - الشريحة التالية، من فضلك.

لذلك NL. هو السجل لهولندا. نحن دولة صغيرة في أوروبا. يمكننا أن نبدأ، على الرغم من ذلك، لأننا وصلنا الأسبوع الماضي إلى علامة 6 ملايين اسم نطاق. لذلك كان هذا رائعًا حقًا وسببًا للاحتفال عبر الإنترنت.

لكن أحد الأشياء المهمة التي نقوم بها هو أننا - إحدى مهامنا المهمة هي أننا نهدف إلى تحسين أمان ومرونة الإنترنت، كما ترون على الشريحة. ولهذا السبب قررنا قبل بضع سنوات البدء في العمل على إنترنت الأشياء خصيصًا لمعالجة بعض التحديات التي تحدثت عنها سابقًا عندما ناقشت الفرص والمخاطر والتحديات في هذا العرض التقديمي.

والسبب في أننا بدأنا في فعل ذلك موجود في الشريحة التالية. إنه في الأساس هجوم Dyn الذي حدث في عام 2016، حيث تعرض مشغل DNS للهجوم من قبل الروبوتات التي أرسلت الكثير من تدفق البيانات. كانت الروبوتات مئات الآلاف من أجهزة إنترنت الأشياء المصابة، وترسل الكثير من تدفق البيانات في نفس الوقت نحو هدفها المحدد. ونتيجة لذلك، تسبب في انقطاع الخدمات الشهيرة مثل Twitter وSpotify وأي شيء آخر.

لذلك عندما رأينا ذلك، اعتقدنا أننا مشغل DNS. نحن بنية تحتية مهمة لهولندا وكذلك للإنترنت بشكل عام، لذلك نريد أن نفعل شيئًا حيال ذلك. هذا عندما بدأنا في تطوير النموذج الأولي SPIN. لذا فإن SPIN هو اختصار للأمان والخصوصية في الشبكات المنزلية.

والغرض من النظام هو المراقبة بشكل أساسي - لذا يمكنك وضع جهاز في شبكتك المنزلية أو تحسين بوابة منزلك، كما تحدث إليوت، مع وظائف أمان إضافية. وستقوم هذه الوظيفة بعد ذلك بمراقبة شبكتك المحلية بحثًا عن أي تدفق بيانات DDOS، على سبيل المثال، لذلك بالنسبة للإشارات التي تشير إلى إصابة أحد أجهزة إنترنت الأشياء الخاصة بك في المنزل بواسطة الروبوتات، على سبيل المثال، وسوف تشارك في إحدى هجمات DDOS الكبيرة.

ما سنحاول فعله بعد ذلك هو محاولة فصل هذا الجهاز مؤقتًا عن الإنترنت لحماية البنية التحتية للإنترنت من هجمات DDOS هذه. لذا فهو نوع من جدار الحماية العكسي، إذا صح التعبير.

وهذا مثال على شيء قمنا بتطويره في SIDN. هذا النظام حاليًا في مرحلة نموذجية، على الرغم من أننا استثمرنا في العام الماضي نوعًا ما في هذا البرنامج للوصول به إلى مستوى الإنتاج لأن ما أردناه هو مساعدة مزودي خدمات الإنترنت ومساعدة مصنعي المعدات الاستهلاكية على استخدام هذه الأنواع من الوظائف على أجهزتهم أيضًا. ولكن تبين أن ذلك أكثر صعوبة مما كنا نعتقد لأنها منظومة مختلفة عن نظام DNS الذي اعتدنا عليه.

وهناك أيضًا - إنها منظومة تجارية مختلفة، إذا جاز التعبير. لذا، على سبيل المثال، مزودي خدمات الإنترنت، على الأقل من تحدثنا إليهم، فإنهم يكافحون من أجل المدى الذي يجب أن يذهبوا إليه لمساعدة عملائهم في حل المشاكل الأمنية لأجهزة إنترنت الأشياء الخاصة بهم التي لم يصدقوا عليها. لذا فهم مترددون نوعًا ما لأن هذه الأنواع من الخدمات الإضافية يمكن أن تسبب عبئًا على دعمهم، على سبيل المثال، مما يقدم تكلفة إضافية. هذا نوع من العوامل التي تجعل نشر هذه الأنواع من النظام صعبًا.

والعامل الآخر هو مصنعي المعدات، وهم في الأساس - يضيفون هذه الوظائف بشكل أساسي إذا طلبها عملاؤهم، إذن مزودو خدمة الإنترنت. لذلك هناك أيضًا مشكلة في الأصل.

نحن نعلم أن هذه مشكلة مهمة، على الرغم من ذلك، إذا نظرت إلى - على الأقل في أوروبا، إذا نظرت إلى هيئة الاتصالات الوطنية الهولندية، فلديهم برنامج محدد حول أمن إنترنت الأشياء. وهناك أيضًا مبادرات في الإعداد الأوروبي حيث يحاول الأشخاص - حيث يحاول مختلف منظمي الاتصالات من داخل أوروبا توسيع توجيه المعدات اللاسلكية الذي هو نظامنا لأي جهاز - يقوم بالإرسال اللاسلكي لتوسيع تلك المواصفات مع المتطلبات الأساسية لأمن إنترنت الأشياء. وهذا يشير إلى أن هذه مشكلة مهمة من منظور عام، إذا جاز التعبير. ولكن هناك المزيد من الجذب الذي يمكن اكتسابه في الصناعة، ولا سيما في عالم ISP. يجب أن أقول عالم الاتصال.

الشريحة التالية من فضلك.

البرنامج الذي رأيته للتو كان مفتوح المصدر. لم تشاهد البرنامج. رأيتم الصورة. عنوان URL، إذا كنت ترغب في الحصول عليه، في الأسفل.

مثال آخر على نفس النموذج الأولي الذي قمنا بتطويره هو زيادة شفافية إنترنت الأشياء. لذا قد تتذكرون أنني تحدثت سابقًا عن فرصة لـ DNS لتصور استعلامات DNS للمستخدمين بطريقة بديهية وسهلة الاستخدام. وقمنا بتطوير نموذج أولي لتوضيح ذلك. هذا ما تراه على هذه الشاشة هنا.

لذا، في الأساس، الدوائر الرمادية، فهي أجهزة في الشبكة. أعتقد أن الجهاز الموجود في الأعلى هو هاتف لأنه يحتوي على العديد من الأجهزة التي يتصل بها.

والأشكال الزرقاء والخضراء، هي في الأساس خدمات عن بعد تتصل بها هذه الأجهزة. هذه لقطة شاشة.

والتطبيق الفعلي ديناميكي للغاية. ترى - في الواقع ترى التفاعلات مع الخدمات البعيدة تظهر عند حدوثها. لذا فإن هذا يعتمد على تحليل استعلامات DNS.

وأود أن أضيف أن SPIN هو حل صديق للخصوصية لأنه يحتفظ بجميع القياسات والتحليلات داخل الشبكة المنزلية. لذلك لا تشاركه مع الخدمات السحابية أو أشياء من هذا القبيل.

حسنًا. إذن كان هذان مثالان، كما تعلمون، للأنظمة التي نحاول من خلالها معالجة التحديات التي تحدثنا عنها في تقرير SSAC.

ثم لدي مثال آخر، وهو في الشريحة التالية.

وهذا المثال الأخير يتعلق حقًا بما قامت به ISOC قبل عامين، وما أسموه بالأمن التعاوني. لذا تعمل العديد من المنظمات معًا لتأمين الإنترنت، وهو أمر ضروري بالفعل للإنترنت لأن الإنترنت هو تعاون كبير. لذلك إذا كنت ترغب في تأمينه، فستحتاج إلى القيام بذلك معًا.

ومن الأمثلة التي نشارك فيها ما تراه هنا. يطلق عليه مقاصة DDOS. والغرض منه - إنه نظام مركزي حاليًا يمكّن الأشخاص من مشاركة ملخصات هجمات DDOS التي عالجوها على أنظمتهم. لذلك يحصلون على تدفق البيانات الواردة. إنهم يولدون بصمة من ذلك، ويشاركون بصمة الإصبع مع مشغلين آخرين داخل تلك المجموعة حتى يعرف هؤلاء المشغلون الآخرون أن هناك - حدث هذا النوع من الهجوم ويمكنهم إعداد بنيتهم التحتية في حالة حدوث الهجوم.

لذا فإن الأمر يتعلق بالفعل بالمبادرة. بالنسبة للضحية، فات الأوان. ولا يزال فعالًا. بالنسبة للأخرى في المجموعة، فهي استباقية لأن لديهم المزيد من المعلومات حول هجمات DDOS والتي قد تحدث في مزودي الخدمة الآخرين.

لذلك هذه هي في الأساس طبقة معلومات ستضيفها فوق البنية التحتية لتخفيف DDOS الحالية. لا يحل محله. إنه نظام إضافي - نظام موزع تضيفه في الأعلى.

وهذا شيء نجربه حاليًا في هولندا. إذن هناك شفرة، نسيت أن أذكرها هنا، تسمى nomoreddos.org. لذا اذهبوا لتفحصه. هناك مدونة تحتوي على معلومات إضافية هناك.

نحن نستكشف حاليًا - نقوم حاليًا بإعداد برنامج تجريبي في هولندا والذي يعد في حد ذاته جزءًا من مشروع أوروبي أكبر يسمى CONCORDIA، والذي يتعلق بالأمن السيبراني بشكل عام. ولكن هناك - ربع هذا المشروع يتعلق حقًا بغرفة تبادل معلومات DDOS.

ونعتقد أن - قمنا حاليًا بتنظيم غرفة مقاصة DDOS بطريقة وطنية. هذا يعني أن الأعضاء هم منظمات من هولندا، مثل الحكومات، ومقدمي خدمات الإنترنت، وتبادل الإنترنت، والسجلات، والعديد من المنظمات. البنوك، على سبيل المثال.

من الممكن أيضًا تنظيمه بطريقة مختلفة. يمكنك أيضًا تخيل غرفة مقاصة DDOS لصناعة نظام اسم النطاق، على سبيل المثال، حيث يتعاون مشغلو نظام اسم النطاق في السجل وربما على مستوى أمين السجل لمشاركة المعلومات حول هجمات DDOS.

هذه في الأساس ثلاثة أمثلة أردت تقديمها من منظور نطاق NL. نأمل أن تساعد في حلها - والمساعدة في معالجة المخاطر واغتنام الفرص التي تحدثنا عنها في تقرير SSAC.

شكرًا.

أليخاندرا رينوسو: شكرًا جزيلاً لك، كريستيان.

الشريحة التالية من فضلك.

حان الوقت الآن لمراجعة الزملاء. يرجى مقابلة المراجعين لدينا. لدينا فيليب فوكوار. إنه ممثل لدائرة موفري خدمات الإنترنت والاتصال ISPCP. فيليب خبير كبير في التسمية والترقيم والعنونة في Orange Labs Networks. منذ عام 2001، كان مسؤول عن أنشطة NN&A داخل Orange Labs لتصميم هندسة شبكات شركة Orange وتقديم الدعم الفني في هذا المجال لوحدات الأعمال داخل المجموعة في جميع أنحاء العالم.

رفيق داماك مهندس كمبيوتر يعمل ويعيش في اليابان بعد أن أنهى درجة الماجستير في علوم الكمبيوتر التطبيقية في جامعة طوكيو. وقد شارك في قضايا المجتمع المدني وحوكمة الإنترنت منذ عام 2007، وحضر العديد من منتديات حوكمة الإنترنت، والمؤتمرات الأخرى المتعلقة بالإنترنت إما كمتحدث أو منظم ورشة عمل.

مجال تركيزه الرئيسي هو في عمليات صنع سياسات ICANN حيث شارك في أدوار مختلفة داخل دائرة المستخدمين غير التجاريين، NCUC، ومجموعة أصحاب المصلحة غير التجارية، NCSG، وعلى تطوير الوعي حول قضايا حوكمة الإنترنت في منطقة الشرق الأوسط وشمال إفريقيا.

كيمبرلي كي سي كلافي هي مديرة مركز تحليل بيانات الإنترنت التطبيقي بجامعة كاليفورنيا في سان دييغو. في عام 2017، حصلت على جائزة الخدمة Jonathan B. Postel وتم إدخالها في قاعة مشاهير الإنترنت في عام 2019. وهي أيضًا أستاذة مساعدة في قسم علوم الكمبيوتر والهندسة في جامعة كاليفورنيا في سان دييغو. تشمل اهتماماتها البحثية طوبولوجيا الإنترنت والتوجيه والأمن والاقتصاد وهيكليات الإنترنت وسياستها المستقبلية. عملت في SSAC في ICANN منذ 2003 وهي حاصلة على دكتوراه في علوم الكمبيوتر من جامعة كاليفورنيا في سان دييغو.

المراجعون الأعزاء، الكلمة لكم.

يمكننا أن نبدأ مع فيليب.

فيليب فوكوارت: شكرًا لك، أليخاندرا. هل يمكنكم سماعي؟

أليخاندرا رينوسو: أجل، نعم.

فيليب فوكوارت: شكرًا لكم، وشكرًا لجميع أعضاء اللجنة. لذا هناك عدد قليل من الطلبات الجاهزة وربما تعليق خاص بي. قدم إليوت حالات استخدام حيث إن إنترنت الأشياء عبارة عن جهاز لخدمة إطار عمل بدلاً من كونه جهازًا لآخر. أفهم أن هناك حجة لوجود بوابة مملوكة لإنترنت الأشياء للشبكة المحلية ليست محجوبة تمامًا عن طلبات DNS الصادرة والواردة، والسبب هو أن تصفية الدخول يمكن استخدامها لتقليل عدد من التهديدات الأمنية.

ليز، لقد ميزت بين البعدين اللذين نراهما في شبكات المحمول 5G، أحدهما هو إنترنت الأشياء على الإنترنت عبر الهاتف النقال وتطبيق إنترنت الأشياء والخدمات المقدمة من قبل المشغل. وقلت أن 5G والتقطيع لم يكن تهديدًا للإنترنت الواحد، DNS واحد (غير مسموع). وهناك بنى تستخدم فيها بنية DNS بالفعل في شبكة الهاتف المحمول، وهي مختلفة عن DNS التي نعرفها على الإنترنت. إذن ليس ثمة شيء جديد هناك.

وأخيرًا، ناقش كريستيان التجربة المبدئية لبوابة DNS الخاصة بـ IoT DNS من خلال SPIN في SIDN لمراقبة تدفق بيانات DNS الصادرة؛ على وجه الخصوص، بهدف مكافحة هجمات الحرمان من خدمات DNS.

إذاً هذه هي وجهات نظري عن المحادثات.

تعليق واحد أو سؤال مني عن التحديات. إن إنترنت الأشياء كونه منظومة معقدة للمشغلين الذين قد لا يشاركون في هذه المنظمة أو أولئك المسؤولين عن تحديد المعايير، على سبيل المثال، هناك دائمًا سؤال عام للغاية حول كيفية تعزيز أو تطبيق الممارسات الجيدة لأهداف المشروع بشكل عام ونظام DNS بشكل خاص. وكيف تتواصل مع مجتمع المشغلين هذا.

لذا، ربما بالنسبة لأعضاء فريقنا أو كغذاء للفكر، سأكون مهتمًا بمعرفة المزيد حول الكيفية - ما موقفك في المنظومة، سواء كنت عاملًا، أو سجلًا، أو بائعًا. كيف يمكننا التواصل مع مجتمع صانعي الأجهزة للترويج لتلك الممارسات الجيدة.

شكرًا. الكلمة لك، أليخاندرا.

أليخاندرا رينوسو: شكرا لك، فيليب.

فيما يتعلق بأسئلتكم، أعتقد أن خبرائنا سيفكرون فيها أكثر قليلاً، وإذا تمكنا من المرور عبر المراجعين الآخرين ثم في النهاية نعود إلى أسئلتكم، فسيكون ذلك رائعًا.

هل يمكن أن نسمع من رفيق الآن.

رفيق دماك: حسنًا. شكرًا أليخاندرا والشكر للمتحاورين على العروض.

لذا، لدي أيضًا بعض النصائح وأحاول أن أفهم نوعًا ما هنا ربما النطاق.

لذا أعتقد أن أحد الأسئلة المهمة هو أنه يبدو خارج نطاق اختصاص ICANN وSSAC، ولكن لأن ما يحتويه نظام DNS من تكنولوجيا هنا أو المنظومة التي يمكن أن يوفرها لإنترنت الأشياء IoT فهذا موضوع مثير للاهتمام بالنسبة لنا، ولكن ما يمكنني ملاحظته هو أننا تحدثنا حول كيفية ربما المشغل المختلف، مشغل إنترنت الأشياء، المنظومة والفاعلين المختلفين، ربما هم - كيف يتعين عليهم القيام به فيما يتعلق بتحسين الأمن والسلامة، لم يكن من الواضح بالنسبة لي ما يمكن أن يكون دور المستخدم. وربما ليس الأمر بهذه البساطة، ولكن ما الذي نتوقعه من المستخدم؟ ما نوع الوعي الذي نحتاجه إلى جانبهم كمستهلك لتلك التكنولوجيا المختلفة؟ في بعض الأحيان، فإنهم حتى يتأثرون بهذه التكنولوجيا، أعني، عندما نتحدث عن إنترنت الأشياء وجميع تلك الأجهزة المنزلية الذكية حيث لا تكون مستهلكًا مباشرًا.

عندما - أعتقد أن كريستيان تحدث عن كيف نحتاج إلى المساعدة فيما يتعلق بالاستخدام، ربما هذه هي صياغتي هنا، بحكمة DNS وأفضل الممارسات. أتساءل، من التجربة الخاصة في ICANN، مثل عندما قدمنا نطاقات gTLD وIDN الجديدة وكانت لدينا تلك الخبرة حول القبول الشامل، كيف يمكن أن يكون ذلك مفيدًا أو مناسبًا بالنسبة للمتعلم (صوتي) - متعلم الاستماع أو نهج، أيضًا، يمكن الاستفادة منه للمساعدة في الانتشار أو استخدام المزيد حول الاستخدام الأفضل أو أفضل الممارسات المتعلقة بنظام DNS وسياق إنترنت الأشياء.

لذا أتساءل عما إذا كان كريستيان ربما، بناءً على تجربته الخاصة وأيضًا مع ما - عمل على نطاق .NL، يمكنه تطوير ذلك ومعرفة ما إذا كانت هناك أي مجالات مشتركة وما يمكننا تعلمه من تلك التجربة.

ربما نقطة أخرى. أعتقد أنه كان من الجيد سماع المزيد عن 5G وكيف أنها مفيدة - في سياق إنترنت الأشياء. وربما لمعرفة كيفية استخدام DNS في ذلك - في هذا المجال. ولكن ربما إذا كان بإمكان ليز أن تتوسع أكثر إلى حد ما إذا كان هناك أي مجال للسياسة نحتاج إلى إدراكه فيما يتعلق بـ 5G.

وهذا كل شيء. هذا من وجهة نظري.

شكرًا.

أليخاندرا رينوسو: شكرًا لك، رفيق. كما قلت، دعنا نراجع جميع المراجعين أولاً، وبعد ذلك سيتم الرد على الأسئلة لاحقًا.

كي سي، تفضلي.

كي سي كلافي: مرحبًا بكم. نعم، كانت تلك العروض رائعة. أنا حقًا أقدر العمل الذي ذهب إليهم وأنا مهتم بشكل خاص بعمل SPIN الذي قامت به SIDN - الذي تبذل الجهد فيه.

أشعر بالفضول لمعرفة ما يعرفه الناس عن دعم الحكومة لهذا النوع من النشاط. أعلم في الولايات المتحدة، أن المعهد القومي للمعايير والتقنية يعمل في هذا المجال منذ سنوات، وأعتقد أني أرى قطارًا قادمًا وأريد مساعدة الصناعة في تجاوز بعض هذه المشكلات. ما أراه هو أن حركة إنترنت الأشياء تفرض - أو ستفرض، ربما لم نر حتى الآن مواجهة مع الفشل في التغلب على العديد من التحديات الأمنية الأساسية المضمنة في بنية الإنترنت. وقد أمضينا الكثير من الوقت وتقنيات تطوير الطاقة مثل DNSSEC وBGPSEC حيث تحاول منظمات المعايير بناء تحسين بروتوكول من شأنه حل مشكلة أمنية محددة ولكنها تتطلب نشرًا عالميًا لم يحدث للأسف حقًا.

كانت المناهج البديلة هي محاولة اقتراح الممارسات التشغيلية مثل، على سبيل المثال، في فضاء BGP، أو MANRS، والتي تعني القواعد المؤكدة المتبادلة فيما يتعلق بالأمن. في الأساس، القواعد السلوكية في عالم ISP إذا فعلت هذه المجموعة من الأشياء، فسوف تقلل من سطح الهجوم من نقاط الضعف الخاصة بأمن توجيه مسار البيانات التي تم بناؤها والتي لم نتمكن من التغلب عليها. هذه التقنية.

أنا أتساءل عما إذا كان بإمكان أعضاء اللجنة التحدث قليلاً عما إذا كانوا يعتقدون أن شيئًا كهذا ذا قيمة في فضاء إنترنت الأشياء، حيث إنه في فضاء إنترنت الأشياء، فإنه ليس حتى من

الممكن إنشاء تراكب تقني بالطريقة التي حاولنا القيام بها في بروتوكولات التوجيه والتسمية نظرًا لوجود العديد من بروتوكولات إنترنت الأشياء المختلفة التي، كما تعلمون، غير قابلة للتشغيل المتبادل. لذا سأكون فضوليًا بشأن بعض الأفكار حول ذلك.

وهذا كل ما عندي. عمل رائع يا رفاق.

سأضع بعض عناوين URL في دردشة عمل NIST.

أليخاندرا رينوسو: شكرًا جزيلاً لك، كي سي.

إذن، الخبراء، من يود أن يبدأ؟

إليوت لير: هذا إليوت.

أليخاندرا رينوسو: تفضل.

إليوت لير: بادئ ذي بدء، نقاط رائعة من قبل جميع المراجعين، وشكرًا لك - ومحادثة رائعة في غرفة الدردشة. إنها في الواقع مناقشة جذابة للغاية.

كي سي محقة تمامًا في أن المعهد القومي للمعايير والتقنية (NIST) كان يقضي الكثير من الوقت والجهد في مواجهة تحديات أمن إنترنت الأشياء، وهي متنوعة وكثيرة. لذلك هناك، على سبيل المثال، NIST TR8228 الذي يتحدث عن اعتبارات إدارة إنترنت الأشياء، وممارسات ومخاطر الأمن السيبراني. هناك أيضًا مسودة التوصية SP1800-15 التي تبحث في إدارة هجمات الحرمان من الخدمات في إنترنت الأشياء مع التركيز على أوصاف استخدام التصنيع.

نقطة واحدة، وبعد ذلك سوف أترك الكلمة، وهي أن إنترنت الأشياء ليست - هي شيء غامض للغاية. يمس قطاعات مختلفة. لقد ركزنا كثيرًا على المستهلكين، ولكن هناك صناعة، ومدينة ذكية، وهناك رعاية صحية. ومن المهم إدراك أن العديد من هذه القطاعات تخضع لتنظيم عالي بالفعل.

ولإعطاء مثال واحد، تقوم إدارة الغذاء والدواء الأمريكية (FDA) بتنظيم جميع الأجهزة الطبية العلاجية، بغض النظر عما إذا كان هناك اتصال بالإنترنت أم لا، فهي تنظم، وسيكون لديها الكثير لتقوله عن أمان الجهاز. وينطبق الشيء نفسه على البنية التحتية الحيوية الأخرى. إن إنترنت الأشياء يمس الصناعة النووية. بالطبع هذا عالي التنظيم.

والسؤال هو أي نوع من التنظيم أو أفضل الممارسات المطلوبة للعديد من المجالات الأخرى حيث نشهد استخدامات جديدة لإنترنت الأشياء يمكن تنظيمها بشكل أكثر موثوقية. حتى المستهلكين لديهم فضاء منظم ولكن من المرجح أن يتم تنظيمه.

شكرًا.

أليخاندرا رينوسو: شكرًا لك، إليوت.

ليز فير: مرحبًا، أنا سعيد للحديث بعد ذلك، إذا كنت تريد.

أليخاندرا رينوسو: نعم، ليز.

ليز فير: بالنسبة إلى فيليب، كيف يمكن الوصول إلى السؤال حول المشغلين المختلفين بشكل أفضل، أعتقد أن التعاون أو التقرير من SSAC هو مثال جيد جدًا على كيفية استخدامنا، كشركات الاتصالات، للعودة إلى عملائنا، من الشركات إلى الشركات، ولكن أيضًا للحكومات وغيرها ومناقشة أفضل الممارسات وكيفية تأمين الأشياء على أفضل وجه. لذا أعتقد أن الحوار بين هؤلاء وICANN وSSAC، وفي أوروبا لدينا ENIS (صوتي) و ETSI. وأعتقد أن هذا أمر مهم. لذلك يجب أن يتم ذلك التقاطع. وبصفتنا ETNO، نحن في الواقع نقوم بهذا التقاطع ونستخدم هذا.

بالنسبة إلى رفيق، إذا كانت هناك أي سياسة في المنطقة بشأن DNS و5G، فهناك الكثير من السياسات حول 5G والأمن في أوروبا في الوقت الحالي. ولدينا قانون أمان جديد، والذي يتعلق أيضًا بالجيل 5G ليس وفقًا لنظام اسم النطاق المحدد، ولكن أعتقد أنه كلما تطور 5G، كلما زاد التركيز في الواقع أيضًا على كيفية التعامل مع نظام DNS و إنترنت الأشياء - في منطقة الأمان.

ولدينا ما نسميه مجموعة أدوات أمان 5G، والتي تتواجد كثيرًا على الأجهزة، ولكن أعتقد أن هذا هو تنظيم مهم سينظر أيضًا في الواقع في مجالات DNS.

إلى كي سي، بشأن الفشل في التغلب على المشاكل الأمنية، هذا صحيح. إنها منطقة تتحرك باستمرار حول كيفية تعاملنا مع الأمن لأن التكنولوجيا تتطور بسرعة كبيرة حقًا.

في أوروبا، لدينا ANISA وهي هيئة أمنية من جانب المفوضية الأوروبية. وقد قاموا بالفعل - وقد أنشأوا الآن مجموعة أمنية لأصحاب المصلحة مع جميع أصحاب المصلحة الذين يناقشون توحيد المعايير فيما يتعلق بالأمن. وأنا متأكد تمامًا أن المناطق المحيطة بإنترنت الأشياء ونظام DNS ستكون جزءًا من هذه المناقشة أيضًا. شكرًا.

أليخاندرا رينوسو: شكرا لك، ليز. أقترح - نعم؟

كريستيان هاسلمان: أردت فقط الرد على ما قاله رفيق عن دور المستخدم.

أليخاندرا رينوسو: تفضل، كريستيان.

كريستيان هاسلمان: لم نتطرق لذلك بعد.

أعتقد أنه من الواضح أن المستخدمين جزء مهم من المعادلة لأن هذا في النهاية هو ما نفعله جميعًا. وأعتقد أننا بحاجة إلى تمكين المستخدمين بطريقة أو بأخرى من فهم أفضل لما يحدث

في إنترنت الأشياء حتى يكونوا أكثر وعياً بما يحدث عندما يتفاعلون، عندما يتفاعلون بوعي، مع أجهزة إنترنت الأشياء، على سبيل المثال، يمكن أن يكون تصوراً أو تمثيلًا آخر لمعلوماتهم الشخصية التي يشاركونها حاليًا مع الخدمات عن بُعد على الإنترنت. وقد يثير ذلك في الواقع نقاشًا أو طلبًا من العملاء، إذا أردت، لهذه الأنواع من حلول الأمان التي يمكن أن يلعب فيها DNS دورًا.

أيضًا، أعتقد أنه - من وجهة نظر المواطن، والتي تعرف أيضًا باسم المستخدمين النهائيين، أعتقد أن الحكومات وهيئات السياسات الأخرى تحتاج أيضًا إلى لعب دور هناك. وأنا أرى بالفعل أن هذا يحدث. لذا في هولندا، على سبيل المثال، فإن منظم الاتصالات الهولندي نشط للغاية في هذا المجال. مثل NIST، على سبيل المثال، في الولايات المتحدة ونرى أيضًا أنشطة حول هذا - حول توجيه معدات الراديو في أوروبا التي تحدثت عنها سابقًا. لذلك أعتقد أنه في نهاية المطاف سوف يندرج أيضًا في السياسة حيث ربما يضع الناس من الحكومات وهيئات السياسة مثل ICANN أساسًا معيار الحد الأدنى من الأمن السيبراني الذي يجب تثبيته على أجهزة إنترنت الأشياء.

شكرًا.

أليخاندرا رينوسو: شكرًا جزيلاً لك، كريستيان والجميع.

الآن، سنراجع الأسئلة التي تم إدراجها في قسم الأسئلة والأجوبة. يرجى تذكيرك باستخدام خانة الأسئلة والأجوبة لأسئلتك. لن تتم قراءة الدردشة بصوت عالٍ.

فكيف تقدمنا في الأسئلة والأجوبة؟ ريا؟

ريا أوتانيس: مرحبًا أليخاندرا. لدينا سؤال من أنجي ماتلابينج: هل من المحتمل أن تكون هناك مشكلات في الذاكرة البديلة قدمتها إنترنت الأشياء الأصغر بكثير، مثل الأجهزة القابلة للارتداء فيما يتعلق باستخدام DNSSEC والتشفير لحماية الأجهزة؟

إليوت لير: ربما يمكنني أن أتحدث عن ذلك؟

أليخاندرا رينوسو: تفضل.

إليوت لير: أنجي، شكرًا جزيلاً على السؤال. تواجه إنترنت الأشياء عدة تحديات فيما يتعلق بالتشفير واستخدام الذاكرة. أولها بوضوح عندما تتحدث عن الأجهزة الاستهلاكية والأجهزة الصغيرة الأخرى على وجه الخصوص، تكون الذاكرة في حالة ممتازة. لدي حرفيًا مناقشات مع مطوري إنترنت الأشياء حول أي بايت.

وإذا نظرت إلى المكدسات التي يستخدمونها، فهي مكدسات تشفير متخصصة، مثل OV SSL هو مثال جيد حيث لديهم مكدسات تشفير محسنة للغاية. إذا نظرت إلى حجم طبقة المقابس الآمنة المفتوحة، يمكن أن يصل حجمها إلى أكثر من ميغابايت. في حين أن OV SSL تبدأ بحوالي 14 كيلو بايت فقط لإعطائكم الإحساس بالاختلافات.

ولكن هناك نوع آخر من القلق الناشئ مع إنترنت الأشياء وهي هذه الأجهزة، كما ذكر شخص سابقًا - ذكر كريستيان سابقًا في مقدمته، فهي تستمر لفترة طويلة.

والتشفير - يتغير عالم التشفير على مدى سنوات عديدة. ما اعتقدنا أنه تشفير مقبول قبل خمس سنوات، قبل عشر سنوات هو عرضة للغاية للهجوم. وإذا كنت تفكر في أجهزة مثل رواسب النفط ومنصات النفط حيث تسقط الجهاز على الأرض لمدة 40 عامًا، فتخيل ما - لا تتخيل. تذكر ما كان لدينا قبل 40 عامًا من حيث التكنولوجيا. وتخيل الآن محاولة تحديث جهاز لاستخدام التكنولوجيا الحالية. جهاز يبلغ من العمر 40 عامًا، تخيل تحديث جهاز عمره 40 عامًا. هذا تحدٍ كبير بالنسبة إلى إنترنت الأشياء. وليست هناك حلول بسيطة.

شخص واحد، أعتقد أنه كان دان جير من معهد ماساتشوستس للتكنولوجيا، لديه ورقة رائعة تحدثت عنها، واحدة، تشير إلى أن أجهزة إنترنت الأشياء لديها في الأساس مفتاح حذف عندما لا تعود موجودة على الشبكة. من الواضح أنه ستكون هناك أوقات عندما يكون ذلك ممكنًا وأوقاتًا عندما لا يكون ذلك ممكنًا. لكنها غذاء للفكر. لقد كانت ورقة رائعة. شكرًا.

أليخاندرا رينوسو: شكرًا جزيلاً لك، إليوت. أعتقد أنه لدينا سؤال آخر.

ريا أوتانيس: نعم. بالنسبة للسؤال التالي، هل تعتقد - من أنوبام أغراواك: هل تعتقد أن نظام المعرفات الحالي سيكون قادرًا على تلبية متطلبات الخصوصية في حالة إنترنت الأشياء؟

إليوت لير: أعتقد أنكم تسمعون الكثير من الصمت لأنه سؤال صعب للغاية للإجابة عليه.

كريستيان، من فضلك.

كريستيان هاسلمان: تحدثنا عنه - في الواقع، أعتقد أن هناك جزأين. الأول هو نظام التعريف الذي في هذه الحالة - ما نتحدث عنه هو اسم النطاق كمعرف. بحيث يمكن حمايتها لزيادة خصوصية المستخدم. تحدثنا عن ذلك في وقت مبكر من الحديث.

ولكن، بالطبع، هناك بُعد ثانٍ، وهو نوع المعلومات التي تشاركها أجهزتك مع الخدمات عن بعد، أليس كذلك؟ لذلك يمكن أن يتعلق الأمر بالمحتوى الفعلي، ولكن يمكن أن يكون أيضًا حول أنماط تدفق البيانات لأنه كان هناك بحث حيث سيتمكن الأشخاص من تقييم نوع الجهاز الذي سيكون لديك في منزلك. فقط من خلال النظر إلى نمط تدفق البيانات وليس الكثير عن محتوى تدفق البيانات.

لذلك أعتقد أن هناك أبعادًا مختلفة يجب النظر إليها إذا كنت ترغب في زيادة خصوصية المستخدم. لذا فإن الأمر يتعلق بحماية الرسائل التي نستخدمها لنظام المعرف، في هذه الحالة DNS. ولكنه يتعلق أيضًا بتدفق البيانات الفعلي الذي يتم تبادله، أو ترسله إلى خدمة عن بعد أو الذي تتلقاه منها لحماية تلك المعلومات، سواء من حيث التشفير وربما حتى من حيث التعتيم حيث تحاول إخفاء أي نوع من الأجهزة يتفاعل بشكل أساسي مع الخدمة عن بُعد.

أتفق مع إليوت على أنه سؤال معقد.

[ضحكات خافتة]

أليخاندرا رينوسو: شكرًا لكم جزيل الشكر، إليوت وكريستيان. إليوت، أنا لا أعرف إن كنت تريد قول شيء آخر حيال ذلك؟

إليوت لير: كنت سأحاول الإجابة على سؤال نايجل. سأل عن التحديات التي تواجه بروتوكول الإنترنت كآلية تسليم لـ 5G في إنترنت الأشياء في عالم المعايير.

أعتقد أن هناك بعض التحديات لـ 5G. الأساسي هو كيف تحد من سطح التهديد لهذه الأجهزة؟ كيف يقوم المزود - ما هو دور مقدم في الحد من سطح التهديد؟ وكيف - ما هو التفاعل بين نقطة التحكم في الشبكة - والذي يعد في الأساس مرشحًا للحزم - ونظام DNS في عالم قائم على السحابة؟

ونفس القضايا التي تحدثت عنها في المنزل هي أيضًا قضايا يجب معالجتها من قبل مجتمع 5G. وقد بدأنا في إجراء هذه المناقشات، ولكننا في بداية تلك النقطة فقط.

أليخاندرا رينوسو: شكرًا جزيلاً لك، إليوت.

سيكون لدينا سؤال أخير لأن الوقت يداهمنا للأسف.

تفضلي، ريا.

ريا أوتانيس: لدينا سؤال من سوادا هادزوفيتش. إذا كان لدينا مزودي سحابة إنترنت الأشياء، فماذا عن العلاقة مع الضباب والحافة وعقد الضباب؟ وفقًا لـ NIST، تكون عُقد الضباب إما مكونات مادية مثل البوابة، وما إلى ذلك.

إليوت لير: حسنًا. أعتقد أنني سأتحدث في هذا أيضًا.

أليخاندرا رينوسو: شكرًا لك، إليوت.

إليوت لير: شكرًا. حاولت مرة واحدة بالفعل الإجابة عن هذا. لذلك هناك نماذج حوسبة مختلفة لأجهزة إنترنت الأشياء.

كما قلت في أحد الإجابات، تكلفة السلع والخدمات على العقدة الفعلية، إذا استطعنا - يحاول المصنعون إبقاء تلك منخفضة للغاية.

ولكن في بعض الأحيان تريد الحصول عليها - لذا ما يفعلونه هو أنهم ينقلون الكثير من القدرة الضعيفة إلى السحابة القابلة للتطوير بدرجة كبيرة. إذا كانت السحابة - إذا كانت الشركة المصنعة أو داعم الخدمة بحاجة إلى المزيد، فيمكنهم إضافة المزيد كلما وسعوا. السحابة رائعة لذلك.

حيث قد يكون لدى السحابة بعض القيود في وقت الاستجابة حيث تريد - حيث تحتاج إلى قدرات محلية. وهذا هو مفهوم الحوسبة الضبابية.

أود أن أقول إنها منطقة تحتاج إلى المزيد من الاستكشاف. إنه ليس شيئًا ستراه في فضاء المستهلك، ولكنك سترى الكثير من الحوسبة الضبابية في الفضاء الصناعي حيث لديك وحدات تحكم محلية توفر إمكانات إضافية من حيث إجراء المعالجة محليًا وتنسيق الاتصال بين أجهزة إنترنت الأشياء.

هناك الكثير من ذلك بالفعل في المجال الصناعي، ولكنه أيضًا منطقة جاهزة للاستكشاف.

أليخاندرا رينوسو: شكرًا جزيلاً لك، إليوت.

بهذا، سأختتم ما قيل في جمل قليلة جداً. من المهم جدًا بالنسبة لنا أن نستمر في المحادثة فيما يتعلق بالفرص والمخاطر والتحديات التي تنتج عن هذا التفاعل بين DNS وإنترنت الأشياء.

من المهم أن تدرك أن هناك تفاعلًا سلبيًا. وهذا يعني أن المستخدم ليس على دراية بما يحدث مع أجهزتهم. إنه شيء للعمل عليه.

الخصوصية هي مشكلة، والأمن مشكلة. هناك بعض التحديات فيما يتعلق بتلك. والعمل الذي يمكن لمجتمع ICANN التركيز عليه هو فهم المزيد حول هذه المخاطر والتحديات وكيف يمكن للمنظمات المجتمعية المختلفة واللجان الاستشارية المساهمة في تحقيق تفاعل أفضل بين إنترنت الأشياء ونظام DNS.

أود أن أشكر جميع أعضاء اللجنة والمراجعين لوقتهم وتعاونهم وكذلك جميع موظفي ICANN الذين دعموا هذه الجلسة العامة. عمل رائع من الجميع.

لقد انتهت هذه الجلسة العامة. شكراً جزيلاً لكم على الحضور. أراكم في الاجتماع التالي.

إلى اللقاء.

[إنتهاء التدوين]