جوهانسبرغ - جلسة اللجنة الاستشارية الحكومية GAC حول استبدال مفتاح التوقيع الرئيسي KSK
الخميس، 29 يونيو 2017 – من الساعة 12:00 م إلى الساعة 12:30 م بتوقيت جوهانسبرغ
ICANN59 | جوهانسبرغ، جنوب أفريقيا

الرئيس شنايدر: لدينا عنصر آخر قبل استراحة الغداء، والذي هو حول استبدال مفتاح التوقيع الرئيسي KSK. قطعة هامة من المعلومات التي أرادت ICANN مشاركتها معنا، ولدينا ديفيد كونراد هنا الذي سوف يقدم نفسه في بضع ثوان ويقول لنا لماذا هو هنا.

متحدث لم يذكر أسمه: (بعيدًا عن الميكروفون).

الرئيس شنايدر: نعم، نعم، فقط خذ أي مقعد، أو يمكنك أيضا أن تأتي هنا إلى الوسط، يا ديفيد.

ديفيد كونراد: مرحبا، بالجميع، أنا ديفيد كونراد، ICANN CTO، وأنا هنا لأتحدث إليكم حول استبدال مفتاح التوقيع الرئيسي الذي نحن بصدد القيام به الآن. مفتاح التوقيع الرئيسي هو المفتاح الذي نستخدمه في DNSSEC لتوقيع شيء يسمى مفتاح توقيع المنطقة. يتم استخدام مفتاح توقيع المنطقة في الواقع من أجل توقيع منطقة الجذر. هكذا يتم تنفيذ DNSSEC. وفي عام 2010، عندما وقعنا الجذر للمرة الأولى، أخبرنا المجتمع أنه بعد خمس سنوات سوف نغير المفتاح، والذي يعرف باسم استبدال المفتاح. والآن نحن في 2017 ونحن في عملية القيام بذلك التغيير. لذا بمجرد تعاون أدوبي، سآخذ عدد قليل من الشرائح لأظهر لكم.

هذا الحديث مقصود أن يكون على مستوى عال حتى تتمكنوا من الفهم. لقد أرسلنا رسالة إلى المنظمين عبر 180 بلدا، وأرسلنا نسخة منه لممثلي GAC لتلك البلدان حيثما كان ذلك ملائما. وفي تلك الرسالة كنا ننوي فقط تنبيه المنظمين بأن استبدال المفتاح قادم وأن عليهم الاستفسار داخل مشغلي الشبكات لديهم إذا كانوا مستعدين لهذا التغيير.

ملاحظة: ما يلي عبارة عن تفريغ ملف صوتي إلى وثيقة نصية/وورد. فرغم الالتزام بمعيار الدقة عند التفريغ إلى حد كبير، إلا أن النص يمكن أن يكون غير كامل ودقيق بسبب ضعف الصوت والتصحيحات النحوية. وينشر هذا الملف كوسيلة مساعدة لملف الصوت الأصلي،إلا أنه ينبغي ألا يؤخذ كسجل رسمي.

لذا مجرد لمحة عامة. لذا فإن مفتاح التوقيع الرئيسي لمنطقة الجذر DNSSEC هو مفتاح التشفير الأعلى المستخدم لتأمين البيانات داخل DNS. وهو يتألف من جزء عام وجزء خاص. ويتم الاحتفاظ بالجزء الخاص فيما يعرف بمرافق الإدارة الرئيسية. فهناك اثنين منهم. واحد على الساحل الشرقي للولايات المتحدة والثاني على الساحل الغربي للولايات المتحدة.

تم تأسيسهم مرة أخرى في عام 2009 عندما عقدنا عقدًا مع وزارة التجارة الأمريكية. داخل هذه المرافق هناك - هو - مستوى عال نسبيا من الأمن. هناك غرفة آمنة. داخل الغرفة الآمنة، هناك قفص آمن. داخل القفص الآمن، هناك خزانة. وداخل الخزانة هناك ما يعرف باسم وحدات أمن الأجهزة. هذه أجهزة متخصصة تحمل معلومات التشفير. لذلك يتم الاحتفاظ بالمفتاح الخاص لمنطقة الجذر ضمن هذا - HSM، داخل الخزانة، داخل القفص، داخل غرفة آمنة، داخل مرافق الموقع المشترك التي لديها تحكم في الوصول.

يتم نسخ الجزء العام من زوج المفاتيح الخاص / العام هذا في كل أداة حل DNS تقوم بالتحقق من صحة DNSSEC على كوكب الأرض. ونحن نقدر أنهم على الترتيب ربما 100 مليون أداة حل على هذا الكوكب، والتي لا تقوم سوى نسبة صغيرة منها في الواقع بالتحقق من صحة DNSSEC . ولكن ما زلنا نتحدث عن ترتيب الملايين من أدوات الحلول هذه التي لديها معلومات التكوين هذه داخلها. استبدال المفتاح هو - آسف، يتم استخدام المفتاح في DNSSEC لبناء سلسلة من الثقة من جذر DNS وصولا إلى - عقدة النهاية، ورقة شجرة التي يبحث عنها في الواقع، وتضمن أن البيانات التي وقعتها DNSSEC من قبل مالك المنطقة، ليست-- لا يمكن تعديلها في رحلة للسماح لأشياء مثل رجل في منتصف الهجمات والتصيد الاحتيالي وهذا النوع من الأشياء. الشريحة التالية من فضلك.

فلماذا نحن نقوم باستبدال المفتاح؟ حسنا، أفضل الممارسات الأمنية الشائعة هي أنه إذا كان لديك كلمة مرور تريد تغييرها من الآن فصاعدا لمنع الحالات التي يتم فيها اختراق كلمة المرور الخاصة بك دون علمك ولضمان أن البنية التحتية اللازمة لتغيير كلمة

المرور تعمل فعلا في الحدث الذي تضطر فيه لتغيير كلمة المرور لبعض الأسباب غير المعروفة.

نفس هذا الأمر صحيح مع DNSSEC. يمكنك التفكير في مفتاح التوقيع الرئيسي ككلمة سر لـ DNSSEC ونتيجة لذلك، نحن بحاجة إلى التأكد من أن البنية التحتية الموجودة لتغيير المفتاح تعمل بالفعل، إذا تم وضعنا في أي موضع قد نحتاج فيه إلى تغيير المفتاح. نحن، كما تعلمون، قد نحتاج إلى تغيير المفتاح إذا كان هناك بعض تكنولوجيا الاختراق التي تسمح بالتحليل إلى عوامل، كما تعلمون، معلومات التشفير أو أن لدينا مؤشرًا على أن - المفتاح قد تم اختراقه في بعض الحالات- بطريقة أو بأخرى. والمشكلة هي أنه نظرا لعدد الأجهزة هناك سيكون لدينا تحديث، يجب علينا أن نفعل ذلك بعناية فائقة، ببطء شديد. نحن - وكذلك نفضل عدم قطع الإنترنت بينما نقوم بذلك. المشكلة هي أننا إذا ارتكبنا خطأ أثناء الاستبدال، فهذا يعني أن أدوات الحلول، والآلات، والخوادم التي يطلب المستخدمون النهائيون البحث عن أي اسم على الإنترنت، سوف يتوقفون تلقائيا عن العمل في أي منطقة موقعة وحيث أن منطقة الجذر موقعة، فهذا النوع من الوسائل سيكون يوما سيئا بالفعل لأي شخص على شبكة الإنترنت. لذلك نحن نفضل عدم القيام بذلك. لذا، فإننا نتخذ نهجا متأنيا ومتعمدا جدا، مع إجراء أكبر قدر من الاختبارات التي يمكننا القيام بها، لضمان عدم وجود مخاطر كبيرة في التسبب في مشكلة في التحقق من DNSSEC عبر الإنترنت. لذلك في الواقع فهي عملية من سنتين ونصف في الأساس. الشريحة التالية من فضلك.

ها نحن ذا. وهذه هي بعض التواريخ الهامة التي حدثت لاستبدال المفتاح، أو التي ستحدث في المستقبل. في 19 أيلول/سبتمبر، تم زيادة حجم المفتاح لأننا في الواقع أدرجنا المفتاح الجديد في DNS لاستخدامه في ما يلي ما يسمى الاحتفالات الرئيسية. الحفل الرئيسي هو عندما نأخذ - نذهب إلى هذه المرافق الآمنة، ونأخذ المفتاح الخاص ونوقع مفتاح توقيع المنطقة من فـVeriSign لاستخدامه للتوقيع على منطقة الجذر. نحن نقوم بذلك كل ثلاثة أشهر. وهذا يعني أن جميع هذه الأنشطة، قد سجلت أساسا على الإدارة الرئيسية الربع سنوية- الاحتفالات الرئيسية التي نقوم بها. وبالتالي فإن آخرها كان في سبتمبر - أو في 27 أيلول/سبتمبر - 19 أيلول/سبتمبر من عام 2017، وحجم مفتاح

DNS سوف يصبح أكبر، لأننا نقوم بإضافة مفتاح جديد. في 11 تشرين الأول / أكتوبر من هذا العام، سنستخدم هذا المفتاح للمرة الأولى.

وهذا نوع من التاريخ الأكثر احتمالا حيث يمكن أن يحدث شيء غريب، حيث الغريب هو أن الناس الذين لم يغيروا مفتاحهم بحلول 11 تشرين الأول/أكتوبر في أدوات الحلول، لن يكونوا قادرين على التحقق من صحتها. سيؤدي أي بحث اسم نطاق يقومون به إلى صفحة "المضيف غير موجود" أو خطأ 404، وهذا النوع من الأشياء.

11 كانون الثاني/يناير نحن في الواقع نأخذ المفتاح القديم ونظل عليه قليلاً حتى نقول أنه لن يستخدم بعد ذلك. في 22 آذار/مارس نحن في الواقع نسحب المفتاح القديم من منطقة الجذر. ثم في آب/أغسطس من عام 2018، ندمر في الواقع هذا المفتاح القديم فقط للتأكد من أن كل شيء يتم الاحتفاظ به بأمان.

الشريحة التالية.

من الذي سوف يتأثر بذلك؟ حسنا، مطوري برامج DNS والموزعين الذين بحاجة إلى وضع المفتاح الجديد في برامجهم وتوزيعها. العاملون على تكامل النظام، يجب على الأشخاص الذين يأخذون البرنامج وينشرونه أن يتأكدوا من أن لديهم أحدث مفتاح ضمن الأنظمة التي يدمجونها. مشغلي الشبكات هم عادة الأشخاص الذين يديرون أدوات الحلول. ويحتاجون إلى التأكد من أن نظمهم يمكن أن تدعم هذا التغيير في المفتاح.

يجب على مشغلي خادم الجذر أن يكونوا على علم، وكنا على اتصال وثيق يهم لأنهم هم الذين سيشهدون على الأرجح المشكلات إذا لم يقم الناس بتغيير المفتاح. ما سيحدث بشكل عام هو أن أدوات الحلول سوف تحاول عدة مرات للحصول على - لحل شيء ما في حالة فشل التحقق من DNSSEC. لذلك سيشهدون زيادة في عدد الزيارات.

مقدمي خدمة الإنترنت هم الأشخاص الذين هم على الأرجح تقريبا - من المؤكد تقريبا سوف يحصلون على المكالمات الهاتفية. إذا كان هناك نوع من المشكلة إذا لم يقم مشغلي الشبكات بتحديث - المفتاح، فإن مقدمي خدمات الإنترنت هم الذين سوف يبدؤون في الحصول على المكالمات.

وسوف يتأثر المستخدمين النهائيين إذا كان مشغل الشبكة لا يقوم بتحديث المفتاح لأنه فجأة أنها لن يكونوا قادرين على الوصول إلى أي موقع على شبكة الإنترنت.

الشريحة التالية من فضلك.

لذلك من الواضح أننا بحاجة إلى القيام بالكثير من التحضير. لقد كنا نطلب من مشغلي الشبكات معرفة ما إذا كانوا قد قاموا بتشغيل التحقق من DNSSEC أم لا. إذا كانوا قد قاموا بذلك، فهم بحاجة للتأكد من أنهم قادرين على تحديث هذا المفتاح. تاريخيا، كانت أدوات الحلول نوعًا من بدء التشغيل، لم يكن عليك أن تفكر في الأمر مرة أخرى، والناس سوف ينشرونه على أنظمة ملفات للقراءة فقط التي من شأنها أن تكون نوعا من المشكلة إذا حاولت تغيير المفتاح لأنك لن تكون قادرًا على الكتابة إلى القرص.

الشريحة التالية.

لذلك ما الذي يحتاج مشغلي أدوات الحلول للقيام به؟ يجب أن يكونوا على علم بما إذا تم تمكين DNSSEC. يتعين عليهم التأكد من فهمهم لكيفية تقييم الثقة عبر أنظمتهم. يحتاجون إلى اختبار والتحقق من أن أدوات الحلول لديهم قادرة على التعامل مع تغيير المفتاح، وفحص ملفات التكوين، التأكد من كتابة الأشياء في المكان الصحيح. وإذا تم تمكين أو التحقق من صحة DNSSEC داخل الشبكة، يمكنك الحصول على خطة للمشاركة في استبدال المفتاح. على سبيل المثال، شاهد السلوكيات في 11 تشرين الأول/أكتوبر وتعرف كيف ستفشل الأمور على الأرجح. وعادة فإن أدوات الحلول التي لم تحدث مفتاحها سوف تبدأ في الرد بفشل الخادم إلى - إشارة فشل الخادم، في أي وقت يصدر فيه شخص ما استعلام عن الاسم الذي تم تأمينه.

الشريحة التالية من فضلك.

هذا للأسف. المربع الأزرق الصغير هناك في الواقع صورة من الرسالة التي أرسلناها. ولكن كما ذكرت، قمنا بإرسال رسالة إلى المنظمين داخل البلدان وممثلي GAC أشاروا أساسا إلى تحدثهم مع مشغلي الشبكات للتأكد من أنهم على بينة من استبدال المفتاح. الشريحة التالية.

وهذا ما أردت توضيحه إلى حد كبير. يسرني أن أتطرق إلى أي أسئلة ويسرني تقديم أي معلومات أستطيع مساعدتكم فيها لمناقشة هذا الأمر مع مشغلي الشبكات. مرة أخرى، أنا ديفيد كونراد، david.conrad@icann.org. وأشكركم على الوقت لتقديم ذلك.

الرئيس شنايدر: شكراً لك ديفيد. حسنًا، أعتقد أن سؤالي الأول هو: هل يوجد رقم هاتف تناظري يمكنك تقديمه في حالة انهيار الإنترنت بأكمله حيث يمكننا طلب المساعدة؟ وهل سيعمل هذا طوال الوقت؟

الولايات المتحدة لديها سؤال أو تعليق.

ديفيد كونراد: للإجابة عن هذا السؤال، نعم، يوجد لدى مركز الدعم العالمي لـICANN معرفة بهذا، ولدينا تلك الأرقام التي تم نشرها في أماكن مختلفة.

ممثل الولايات المتحدة الأمريكية: شكراً لك ديفيد. كان هذا عرضًا مفيدًا للغاية. هذه مسألة قريبة وعزيزة على قلبي لأنني أحفظ كثيرًا في قلبي، فيما أعتقد. ولكننا تلقينا الخطاب من غوران. شكرًا جزيلاً. وسأكون صادقا معك، كان رد فعلي الأول هو أننا بحاجة إلى العمل مع مزودي خدمة الإنترنت لدينا. وكحكومة، نعتمد عادة على قراراتنا - قرارنا مع مقدمي خدمات الإنترنت التجارية.

ولكن من حيث توفير التوجيه لنا، هل هناك أي شيء نحن بحاجة إلى القيام به كحكومات للتأكد من أن لدينا - بالإضافة إلى مجرد التأكد من أن مقدمي خدمات الإنترنت يفعلون ما يحتاجون إلى القيام به، هل هناك أي شيء توصون بالقيام به داخليا للتأكد من استمرار عملياتنا؟ شكرًا.

ديفيد كونراد: أجل. في أي شبكة، سواء كانت الشبكة الداخلية للحكومة أو شبكة مزود خدمة الإنترنت، هناك حاجة إلى أن يكون هناك أدوات حلول في مكان ما. قد يكون خارجيًا. على سبيل المثال، توفر غوغل خدمة DNS العامة 8.8.8.8. العديد من الأشخاص يستخدمون هذه الخدمة.

كل ما تحتاجه هو التأكد من أنهم قادرين على التعامل مع استبدال المفتاح.

بالتأكيد غوغل قادرة على التعامل مع استبدال المفتاح، كما قيل لي. لا شك لدي حيال ذلك- لا أشك في ذلك مطلقًا.

ولكن بالنسبة لمزودي خدمة الإنترنت الآخرين، وعمليات الشبكة الأخرى، ولا سيما عمليات الشبكة على مستوى المؤسسة، فإنه من الجيد أن - اسأل فقط لمعرفة ما إذا كانوا على علم بأن المفتاح سوف يتغير. وإذا كانوا على علم - حسنا، يجب أن يتحققوا أولاً لمعرفة ما إذا تم تمكين DNSSEC وتشجيع تمكين DNSSEC، إن أمكن. ولكن بعد ذلك إذا تم تمكينه، يجب التحقق لمعرفة ما إذا كانوا على علم بأن المفتاح سوف يتغير. وإذا لم يكنوا كذلك، يقترح أن يشاركوا في جهود استبدال المفتاح التي تقوم ICANN بالإعلان عنها.

ما نقوم به هنا يعكس ما كنا نقوم به في العديد من الأماكن، وأساسا مجرد محاولة لجعل - زيادة الوعي بأن هذا يحدث ولكن من الواضح أننا لن نكون قادرين على لمس الجميع. لذا، فإننا في الواقع نطلب أن تقوم الحكومات، كما تعلمون، ببذل بعض الجهود لجعل مشغلي الشبكات على علم بأن استبدال المفتاح سيحدث.

الرئيس شنايدر: ثم ممثل إيران.

ممثل إيران: شكراً جزيلاً على ذلك العرض التقديمي. هل لديك أي قناة ردود فعل للتأكد من أن الإجراء الذي أشرت إليه، تم تنفيذه على النحو الواجب قبل تقسيم أي شيء؟ ليس الجميع على علم ويتبعون الإجراءات بسرعة. لذا مجرد سؤال حول التعليقات التي، نعم، لقد تلقينا رسالتكم، ونحن ننفذ. ربما تشير إلى أي صعوبات محتملة؟ أو ليس لديكم هذا النظام للتعليقات؟ شكرًا.

ديفيد كونراد: نحن عموما، في جميع الحالات التي كنا، كما تعلمون، تكلمنا، وشجعنا الناس على الاتصال بنا، وطرح أي أسئلة قد تكون لديهم أو أي مخاوف قد يرغبون في التعبير عنها.

ليس لدينا أي آلية واضحة لفرز الأشخاص المطلوبين لتقديم التعليقات. ولكننا نعمل بشكل خاص مع مجموعات عمليات شبكة مختلفة، ومنظمات TLD مختلفة، وهذا النوع من الأشياء، لتوفير مكان حيث، كما تعلمون، يمكن إنشاء قنوات اتصال للسماح بتقديم هذه التغذية لنا.

الرئيس شنايدر: شكرًا. لدي ممثل مصر، النرويج والمملكة المتحدة ثم هولندا، عفوًا.

ممثل مصر: شكرًا لك، توماس. وشكرًا لك ديفيد على هذا العرض. لدي سؤال بشأن الشريحة رقم 5. ولكن في الوقت نفسه، إذا فهمت بشكل صحيح، هناك بعض الأدوات للتحقق من أنك على استعداد ل - وأعتقد أن هذا مفيد لمعرفته.

ديفيد كونراد: نعم. لقد أنشأنا اختبارا سيسمح لمشغلي أدوات الحلول بالمشاركة في اختبار حقيقي لاستبدال مفتاح التوقيع الرئيسي KSK. للأسف فإن الاختبار ليس في هذه الشريحة. كان أكثر توجها إلى سطح الشريحة الأكثر تقنية، ولكن يمكنني تقديم تلك المعلومات إلى أعضاء GAC لتوفيرها لمشغلي الشبكات الخاصة بهم داخل بلدانهم.

ممثل مصر: نعم، شكرًا لك. أعتقد أن هذا مفيد للغاية.

وسؤالي عن الشريحة 5 من فضلك.

فقط للتأكد، هل هذا يؤثر على أدوات الحلول خاصة؟ لأنني لا أرى هنا ccTLD-- أعني، سجلات TLD، المشغلين. لذا فهل هي أدوات الحلول خاصة؟ شكرًا.

ديفيد كونراد: حسنًا. لذا فإن الأشخاص المتأثرين هنا على نوع DNS الذي يجلب المعلومات بالفعل من مشغلي TLD. لن تتأثر نطاقات TLD، وccTLD وgTLD باستبدال المفتاح. وليس عليهم القيام بأي شيء. لا توجد وظائف يوفرونها تأثرت هنا بخلاف، بطبيعة الحال، نظمهم الداخلية وأدوات الحلول التي يشغلونها ضمن نظمهم الداخلية.

الرئيس شنايدر: شكرًا.

هولندا.

ممثل هولندا: نعم، شكرًا لك ديفيد على الشرح الذي قدمته. فقط أريد التأكد من بعض الأشياء. أعتقد أن الحكومات ليس لديها مسؤولية رسمية في هذا الصدد. ولكنك تستخدمهم فقط للتواصل مع مقدمي خدمات الإنترنت. ولكن ليس هناك، دعنا نقول، مسؤولية حكومية؟

ديفيد كونراد: بالضبط. نحن نبحث عن أي قناة اتصال يمكننا لمسها، نعم.

ممثل هولندا: وثانيا، كانت هناك قائمة بأدوات حلول DNS، والمحللين المتكررين، الذين يقومون بالتحقق من صحة DNSSEC في كل حرف. في حالتنا، فالأمر عن سبعة أو ثمانية، فيما أعتقد. وبطبيعة الحال، تم الاتصال مع هذا مباشرة، وأنا أفترض، هؤلاء هم الذين عليهم بالفعل القيام بالتغيير، تغيير حقيقي في أنظمتهم. غير أن جميع أصحاب المصلحة المتأثرين الآخرين لهم تأثير ولكن هل عليهم حقا تغيير أنظمتهم؟ شكرًا.

ديفيد كونراد: وبالتالي فإن الطريقة - العملية الفعلية لكيفية حدوث التغيير الرئيسي سوف تحدث، هناك في الواقع وضع آلي، إذا كنت تقوم بالتشغيل حتى الآن - إذا كان مشغل أدوات الحلول يشغل برنامجًا حديثًا مع تمكين التحديثات التلقائية، فليس عليهم في الواقع القيام بأي شيء. قد يكون من الحكمة المشاركة في الاختبار للتأكد من أنه لا شيء غريب سوف يحدث عندما يحدث بالفعل استبدال المفتاح. ولكن في النهاية هناك أتمتة بنيت في أدواتل الحلول الحديثة التي من شأنها التعامل مع استبدال المفتاح هذا تلقائيا.

إذا لم يتم تشغيل - عذرا، أو عدم تشغيل برنامج جديد أو عدم تشغيل الاستبدال التلقائي، فعليهم تغيير نقطة بيانات التهيئة. إنه بالفعل-- المفتاح العمومي المرتبط بمفتاح التوقيع الرئيسي، سوف يحتاج إلى نسخصه إلى ملف التكوين. لذا، فهذه هي الحالة التي ينبغي على مشغلي أدوات الحلول اتخاذ بعض الإجراءات.

الرئيس شنايدر: شكرًا. المملكة المتحدة، باختصار من فضلك.

ممثل المملكة المتحدة: نعم، شكرًا لك. شكرًا جزيلاً لك ديفيد، على إطلاعنا باختصار حول هذا الموضوع.

لم أتحدث بالفعل إلى أعضاء المملكة المتحدة في دائرة مقدمي خدمات الإنترنت هنا، ISPCP. في الأساس، فهم جميعًا موظفوا اتصال، ولذا فإنني سوف أتحقق. لكنني أفترض أنك سوف تنظر إليهم للقيام بتوعية حرجة جدا، لمزودي خدمة الإنترنت في

جميع أنحاء العالم. هل أنت واثق من أن ذلك سيحدث؟ وسيكون من المفيد جدا الحصول على هذا الطمأنينة.

وفي الواقع أنا لم أر الرسالة لذا لا بد لي من التحقق من ذلك أيضًا. أنا لا أعرف أين قد ينتهي ذلك.

ولكن أعتقد أنني سمعت أيضا أنك تقول أنه سيكون من المفيد بالنسبة لنا التحقق المزدوج مع شبكتنا العالمية - مقدمي الشبكة الحكومية. بالنسبة لي هو مكتب مجلس الوزراء في لندن. ماذا تفعلون في الحادي عشر من تشرين الأول/أكتوبر؟ هل تتطلعون إلى ذلك اليوم؟ أعني، إذا كان هناك شيء قد يحدث خطأ بسبب فشل الناس في إجراء التحول اللازم، إذا كانت هذه هي الكلمة الصحيحة، فهل سيكون هناك أي عودة لنا كحكومات تحمي كيفية حل كل شيء؟ أو كيف تتعامل مع الفشل الكبير في تلك المرحلة في 11 تشرين الأول/أكتوبر؟ نعم، عذرًا.

ديفيد كونراد: لذلك نعم، كنا على اتصال مع ISPCP وشجعناهم على الاتصال بأعضائهم والهيئات الأخرى التي كنا نتعامل عليها- كما تعلمون، الذهاب إلى اجتماعات مجموعة عمليات الشبكة على نطاق واسع جدا.

فيما يتعلق بـ"في حالة حدوث شيء سيء"، نحن - أنشأنا نظام مراقبة متطور جدا لمشاهدة حركة المرور إلى خوادم الجذر التي من شأنها أن تكون نوعا من أول مؤشر على أن الأشياء السيئة تحدث لدينا، ولدينا خطط احتياطية سيتم تنفيذها، إذا كان هناك - اكتشفنا، كما تعلمون، نوعا من الحدث الهام الذي أشار إلى أن الاستبدال قد فشل.

ونحن واثقون إلى حد ما من أنه من غير المحتمل أن تحصل الحكومات على غضب المستخدمين النهائيين ومشغلي الشبكات. وأتوقع أن يكون ذلك في الواقع موجه إلى ICANN أو، بشكل أكثر تحديدا، إليّ، وهذا أحد الأسباب التي جعلتني أشارك بشكل كبير في محاولة الحصول على المعلومات عبر ذلك حيث أنه من المهم حقا أن يقوم الأشخاص بتحديث مفتاحهم.

الرئيس شنايدر: عذرًا. يرجى عدم ترك الغرفة. هناك إعلان هام سوف أعلنه بعد دقيقة واحدة، لذلك اسمحوا لي أن أعطي الكلمة فقط إلى الرجل الذي في الخلف. أعتقد إذا كنت - أنت نيجيريا، هل هذا صحيح؟

ممثل نيجيريا: ممثل نيجيريا، نعم.

الرئيس شنايدر: شكرًا. ورجاءً لا تغادروا الغرفة. هذا هو آخر تدخل سنقوم به ثم علينا أن نتوقف بشدة. بشكل أو بآخر نتوقف تمامًا. ممثل نيجيريا، يرجى المضي قدما.

ممثل نيجيريا: شكرًا على العرض التقديمي حول استبدال DNSSEC.

سؤالي هو أنه بالنسبة لمزودي خدمة الشبكة الذين لم يقوموا بتشغيل DNSSEC، ماذا يحدث لهم بعد الاستبدال؟ إنهم لم يقوموا بتشغيل DNSSEC أصلا على شبكتهم. شكرًا.

ديفيد كونراد: أجل. لن يرون أي تغيير. إذا لم يتم تمكين DNSSEC، فلن يكون لاستبدال المفتاح أي تأثير. إذا قرروا في مرحلة ما في المستقبل تمكين DNSSEC، فسوف يحتاجون إلى التأكد من أن لديهم أحدث مفتاح. إذا لم يفعلوا ذلك، فسوف تفشل عمليات التحقق الخاصة بهم، وسوف - سوف يرتبكون. لذلك هم فقط بحاجة للتأكد من أن لديهم أحدث مفتاح أو أحدث توزيع للبرامج، والتي من شأنها في الواقع على الأرجح جلب أحدث مفتاح تلقائيا.

الرئيس شنايدر: علينا أن نتوقف هنا لأن --هناك العديد يريدون كلمة قصيرة ثم نحن نعلم ما يحدث-- لأن لدينا شيء مهم لنخبركم به. كما تعلمون، هذا هو آخر غداء لنا في هذا الاجتماع، أو وقت الغداء، وهذا يعني أنه آخر وقت غداء لأولوف في وظيفته -

ما هي وظيفتك في الواقع؟ فريق عمل ICANN يدعمون GAC ويطلقون النكات الرائعة في أي وقت من اليوم أو الليل على المكالمات الهاتفية وأيا كان، مثل الدعم ضروري.

في الواقع، جوليا، التي ربما تحتبيء مرة أخرى كالمعتاد في مكان ما، إنها في الواقع كانت تخرج لجلب هذه المنظمة - ساعدتنا في تنظيم هدية صغيرة لأولوف.

[ضحك]

سترون - ونحن سوف نتحقق مع الفنيين حول كيفية جلب ذلك لدينا. هذا فقط-- أعتقد أن هناك بطاقة لذلك، وهذه هي الهدية. انها ليست ثقيلة جدا لذلك يجب أن تعمل في الواقع، لذلك نحن فقط أردنا أساسا مرة أخرى وأخيرا وبالفعل بكل فرحنا أن نقول شكرا لك، أولوف.

وهناك بعض النظارات مختفية في الخلف، لذا فهذه القليل من المشروبات وقليل من الوجبات الخفيفة للاحتفال باللحظات الأخيرة مع أولوف في هذا المنصب. شكرًا جزيلاً، أولوف.

[تصفيق]

أولوف نوردلينغ: شكرًا جزيلاً لكم. أردت دائمًا سندان-

[ضحك]

كحقيبة يد مريحة.

فعلا، لقد كان ذلك رائعًا. شكرًا جزيلاً. و، حسنا، وآمل البقاء على اتصال، على الرغم من أنني سوف أذهب إلى التقاعد وهلم جرا.

لذلك - سوف أظل على مقربة حتى نهاية تموز/يوليو، لذلك - حسنا، لن تتخلصوا مني تماما حتى الآن، ولكن شكرا جزيلا لكم.

الرئيس شنايدر: حسنًا. يمكننا جميعًا الرجوع إلى الخلف--

ممثل البرازيل: توماس، هل يمكنني أن أسألك؟

الرئيس شنايدر: نعم.

ممثل البرازيل: فيما يتعلق بما بعد الغداء، سوف نتقابل هنا ثم لدينا هذا الاسم الجغرافي، ولكن ماذا ننوي؟ لأنني أعتقد أننا بحاجة أيضا في مرحلة ما إلى الاجتماع معا لمناقشة البيان أم أنه لن يكون ضروريا؟ ماذا سيحدث في هذه الحالة؟ لأن الأمس تحدثنا عن الاجتماع في وقت ما في الساعة 3:00 أو مع وجود بعض التفاعل.

الرئيس شنايدر: سنقوم - سوف نرى أجزاء النص التي لدينا-- أو حصلت بالفعل. توم لديه نظرة عامة على هذا. سوف ننظر إلى هذا خلال وقت الغداء في وقت ما ثم بعد - الفكرة هي، في الساعة 3:00، تكون الأمور جاهزة ومن ثم قد تنفق خمس دقائق أو نحو ذلك، ونأمل، وضع اللمسات الأخيرة على هذا. ولكن نشكركم على تذكيرنا.

لذا لا تهربوا بعيدًا. العمل لم ينته بعد. شكرًا.

ولكن أولاً، إنه ليس العمل، إنه الاحتفال بألوف. شكرًا.

[استراحة]