

أبو ظبي - ورشة عمل DNSSEC -- الجزء 1
الأربعاء، الموافق 1 تشرين الثاني (نوفمبر) 2017 - من الساعة 09:00 ص إلى الساعة 10:15 ص بالتوقيت الرسمي الخليجي
ICANN60 | أبو ظبي، الإمارات العربية المتحدة

سيادة غير معروفة:
1 تشرين الثاني (نوفمبر) 2017. القاعة أ القسم ب، ج، ورشة عمل DNSSEC
الجزء 1، 9:00 – 10:15.

روس موندي:
طاب صباحكم جميعاً. مرحبا بكم في ورشة عمل نشر الإمتدادات الامنية لنظام اسم
النطاق DNSSEC. اسمي روس موندي بمعية بارسونز وجاك لاتور وسجل CA
سنكون اليوم المضيفين الأساسيين. ألا تسمعوني؟ قد يكون الأمر كذلك. يتعين عليكم
تحمل الأمر. حسناً.

حسناً. سنعقد جلستنا اليوم. أظن أن هناك وجوه جديدة. هناك وجوه رأيناها من قبل في
ورشة العمل. ونود أن نجعل من هذا الأمر قدر المستطاع نشاطا تفاعليا.

لذا يتعين أن يكون أمام الجميع البرنامج. وخلف البرنامج هناك تذاكر للغذاء خاصة بكم
في حال رغبتكم في البقاء وتناول الغذاء معنا عند الظهيرة. وعندنا وجبة غذاء مجاملة من
رعاتنا. شريحة العرض مع الراعين هي – أجل، ستعرض قريبا.

هؤلاء هم الراعين، حسنا. Afilias، CIRA، SIDN، .ca و dot – حسنا سجل
Afilias. على أي، إنها مجموعة جيدة من الراعين وهذا هو الأمر المهم. لنصفق بحرارة
على تقديم رعاتنا وجبة الغذاء. هناك وجبة غذاء مجانية مخصصة للمشاركين في ورشة
العمل DNSSEC. حسنا، دان يورك هو من يقوم غالبا بهذا الأمر لكن اليوم وعوض
أن يكون عرضا لدان و روس، سيكون عرضا لدان و جاك. اسمي روس. والشخص
الغائب هو دان. لذا سيقوم جاك بالعرض الذي يقوم به عادة دان في البداية. وبهذا سأعطي
الكلمة لجاك.

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.

جاك لاتور:

لنقم بإطلالة على جدول الأعمال. أجل. حسنًا. حسنًا. بالنسبة لليوم، ستكون لدينا مقدمة موحدة حول العالم، وجميع شرائح العرض المقابلة في DNSSEC. وبعدها ستكون لدينا حلقة نقاش بشأن أنشطة DNSSEC مع التركيز على ما هو إقليمي.

ستعالج ورشة العمل الثانية الحالة الراهنة لـ KSK Rollover، وما يليها، وما الذي يحدث. لذا سيكون لدينا نقاش جيد بشأن ذلك. وبعدها سنجري الاختبار المهم DNSSEC/DNS. والكثير من الأشخاص هنا فقط لأجل ذلك. وأنا على يقين تام من ذلك. وبعد وجبة الغداء، ستكون لدينا عدة عروض بشأن أمور تتعلق بـ DNSSEC. وسيكون ذلك موعدا مهما. الشريحة التالية.

حسنًا. حسنا دعونا نجوب حول العالم. الشريحة التالية. حصلت على جهاز التحكم. نعم.

حسنا قامت ISOC بكتابة تقرير نشر DNSSEC لسنة 2016. إذا قمتم بالبحث عن ذلك، ستجدون تقريراً شاملاً نسبياً عن حالة نشر DNSSEC وجميع المبادرات إلى غاية 2016. وبالتالي فقد قام دان والشركة بعمل جيد في إعداد جميع هذه الأمور. لذا إن كنتم ترغبون في معرفة أي شيء بخصوص DNSSEC، فهذه نقطة انطلاق جيدة. إذ يتضمن إحالات كثيرة على الكثير من روابط المعلومات للتعرف أكثر على DNSSEC.

من منكم يحضر لأول مرة ورشة عمل DNSSEC؟ حسنًا، شكرًا. هذا أمر يتعين معرفته. حتى أعرف ما إذا كان بإمكانني أن أقوم بالعرض بوثير سريعة أو بطيئة في حال رأيتم جميعكم أم لا هذا من قبل.

وهذا الأمر مبني على مختبر APNIC. إنه رسم بياني لتحقق DNSSEC على الصعيد العالمي. لذا مع مرور الوقت، كنا نتعقب هذا الأمر. وعندما رأيت الشريحة التي تتضمن الرسم البياني لأول مرة، لاحظت أن هناك تراجعاً ربما في تموز (يوليو). قد تكون لديكم ملاحظات حيال ذلك.

جيف هوستون: قامت دعامة BSNL بتشغيلها - كان ذلك قبل سنة أو ما يقاربها. وفي الهند BSNL كبيرة جدا. وهناك العديد من العملاء. في تموز (يوليو)، قاموا بإغلاقها. وهذا ما أدى إلى وقوع خلل في الأرقام بسبب إغلاقهم لها. ولم أسألهم أبدا عن سبب قيامهم بذلك. هناك سببان محتملان. أولا، لم يكونوا يعرفون أبدا أنهم قاموا بتشغيلها في الأول، وهو ما حدث باليمن. لذا أحيانا فهي تشتغل بمحض الصدفة ويقومون بإغلاقها عندما يدركون ذلك.

والتعليل الآخر المحتمل والأكثر إحباطا هو نظرتهم في قائمة KSK الواردة وقرارهم عدم القيام بالأمر. وليست لدي أدنى فكرة عن السبب الحقيقي من بين هذين التعليلين. في حال حضر معنا شخص ما من الهند وهو على دراية بهذه الحالة بخصوص BSNL، فأرجو أن يخبرني. لكن هذا كل ما أعرفه.

جاك لاتور: شكراً. هل من أحد هنا من الهند؟

شخص غير محدد: أجل، أنا من الهند، لكن ليس لدي أي مستجد في هذا الشأن. لذا لا نعرف إن [كان هناك هذا الأمر] بخصوص BSNL [غير مسموع] وجميع الأمور.

جاك لاتور: حسنا هذا ما أقترحه عليكم. ابعثوا بريد الكتروني كي نعلم أي سيناريو كان ذلك. لا أعرف إن كانت مشغلة أو يا إلهي، يجب علي إغلاقها. حسناً. بخلاف ذلك، فهي تعرف نسبيا نمو مطردا، نمو مطردا بطيئا. هذا هو موقفنا.

لذا إقليميا، فالرقم واحد هي جنوب إفريقيا بنسبة 38% DNSSEC وبعدها تتراجع النسبة إلى 2%. الأمر الجيد أن الرقم المعتمد عليه في DNS العام لـ Google ليس بهذا الارتفاع. تعتبر الأقاليم الأكثر ارتفاعا.

وهذا يعني أنكم تديرون بنيتكم التحتية ولا تعتمدون كلياً على Google للعمل DNS الخاص بكم. لذا فالأمر في تحسن. في ما يخص تحقق DNSSEC لآسيا، فلدينا العراق بنسبة 57% و 25% على Google. هذا جيد للغاية. وتراجع تلك النسبة لتصل 0% في الكويت، لذا يتعين القيام بعمل ما إما قبل أو بعد استبدال KSK. يتعين علينا التفكير في تشغيل التحقق هنا. وسيكون ذلك فرصة جيدة.

في ما يخص نشر TLD حول العالم، ما زلنا عند نسبة 90%، وهي صعبة القراءة. 90% من جميع TLD ومنطقة الجذر تم توقيعها. وحوالي 4% من مستوى النطاق الثانوي قبل ذلك تم توقيعها. وما مجموعه 13% من المستخدمين هم في طور التحقق. وهذه أرقام مهمة يتعين الاحتفاظ بها وتذكرها. وهذا عمل كبير بناء على بحث قام به ريك لامب على إحصائيات DNSSEC. وأظن أن الحصول على 10% الأخرى يتطلب بعض الوقت لكن العمل في طور الإنجاز.

وهو أعلى رقم موقع لنطاقات TLD. إذن الأمر هو TLDs بالنطاقات الأكثر توقيعاً. يا إلهي، هذا قليل. فـ .nl بنسبة 48% من النطاقات تم توقيعها. أي 2.8 مليون على 5.7 مليون نطاق، وهذا أمر جيد. وبعدها البرازيل بنسبة 23% - من إجمالي عدد النطاقات، أي حوالي مليون نطاق تم توقيعها. وبعدها تتراجع. في .ca. عندنا 500 لذا أظن أنه علينا التقدم قليلاً قبل الدخول في نطاق المليون. فالجديد إذن يا ريك ليس هو تعقب عدد النطاق باستخدام خوارزمية تشفير خاصة لـ DNSSEC. لذا إن كنتم تودون معرفة أكثر بشأن ذلك، فتستطيعون زيارة موقعه الإلكتروني والحصول على المزيد من الإحصائيات. ولكل من يود التحدث مع ريك فهو هناك.

الآن سننظر في تنفيذ TLD على مستوى الإقليم. لدينا خمس حالات مختلفة، ودان يتعقب حالة كل TLD بناء على ما إذا كانوا يقومون باختبار داخلي باستخدام DNSSEC، وما إذا قاموا بالتزام عام بنشر DNSSEC بمنطقتهم حيث تم التوقيع عليه، لكنه لا يشتغل. وقد حصلوا على تقنية التوقيع عليه. DNS هو في الجذر، ما يعني تم التوقيع عليه، وهناك سلسلة ثقة لكن لا أحد من أمناء السجل سبق أن وافق على سجل DS. وبعدها مرحلة التشغيل التي تعني الموافقة التامة على تفويض الدخول إلى السجل بواسطة APP.

لذا فأغلب هذا الأمر تم القيام به يدويا كونه ليس أمرا نستطيع القيام باستفتاء بشأنه كي يشتغل، بل يكون على أساس المناقشة. وهو مبني على جواب TLDS على متى يعتزمون القيام فعلا بأمر ما، ويخبرون دان يورك حتى تقوم بتحيين إحصائياتنا. هكذا يجري الأمر.

وبناء على هذا، يستخرج دان خرائط العالم والحالة الراهنة. وخلال الخمس سنوات الماضية حققنا تقدما جيدا نسبيا. وأعتقد أن ما يتعين القيام به هو الرجوع إلى الحالة التي كنا فيها قبل سنة أو سنتين والقيام بمقارنة. حتى يتضح أننا نحقق فعلا تقدما جيدا. فسابقا كان هناك كثرة الأصفر والأحمر وهو أمر يتحسن. للإشارة هناك DS 46 في الجذر ما يعني الحصول على أمين السجل، والعمل مع أمين السجل للموافقة على مفاتيح DNSSEC يبدو تحديا لبعض TLDS وهذا أمر يتعين علينا النظر فيه.

ففي منطقة إفريقيا، حيث تظهر الحالة الراهنة في المنطقة بناء على اللون. فغينيا بيساو GW. تم تخصيصه في تشرين الأول (أكتوبر) وجنوب إفريقيا ZA. تم تشغيله وهذا أمر جيد. وهذه أمور يتعين تذكرها في النهاية. ماذا؟ نحتاج إلى تذكرها. وفي آسيا، SA. مشغل، وهذا أمر عظيم. وهذا أمر يستحق منا أن نخصه بتصفيق حار. هذا جيد. لذا نسبيا فهو نفس السيناريو. 24 مشغل، DS 17 بالجذر.

هل من أحد هنا لديه DS بالجذر؟ ما الذي يمنعه من التشغيل الكامل؟ هل من أحد هنا منتم لإحدى هذه TLD؟ لا، نعم؟ أم أننا في الحقيقة لسنا على علم بتحديث التشغيل الخاص بكم؟ حسنا. سأطرح السؤال لاحقا عند استيقاظ الأشخاص.

وفي أوروبا، قمنا بإضافة ألاند، وهذا بالنسبة لي شبيه بجزيرة AX. في آب (غشت). وتنقصنا ايطاليا، لست متأكدا من الحالتين الآخرين. أي واحدة؟

[غير مسموع]

شخص غير محدد:

جاك لاتور:

حسناً. هناك تقدم إذن. مثل TLD، فالأرجنتين مازال يتعين القيام بأمر ما. فالصورة لا تزال نسبياً مماثلة لما كانت عليه من قبل. وقد تمت إضافة برمودا في حزيران (يونيو). مازال هناك عمل يتعين القيام به. وبدخول غرينلاند. ليس هناك أي DS بالجذر. وقد التقينا في الحقيقة بشخص من غرينلاند وهذا أمر جيد. نحن على علم بوجودهم.

إن كنتم مهتمين، فهذه الأمور، هذه الخرائط وجميع صور jpeg يمكن بعثها عن طريق البريد الإلكتروني – في حال تسجيلكم بتلك اللائحة، فستحصلون على ذلك مرة واحدة كل شهر، مجموعة كاملة من الخرائط وجميع التغييرات. لذا عند قيامكم ببعض الأبحاث في DNSSEC، تستطيعون استخدام تلك المعلومات. وهذا أمر مبني أساساً على التحيينات التي قام بها دان.

هناك مشروع مستمر للسجل الزمني لـ DNSSEC. لذا تستطيعون الرجوع إلى الحالة الراهنة. وهناك رابط URL الخاص بها. ويعمل دان والشركة على ذلك. تستطيعون معرفة أين كنا من قبل، وهم بحاجة إلى المحتوى، وهذا ما يطلبونه. إن كانت لديكم أي معلومة مفيدة بشأن نشر DNSSEC، تستطيعون الذهاب وتسجيل الدخول هناك والمساهمة في مشروع السجل الزمني. وهذا كل ما في الأمر. هل من أسئلة؟

جولي هيدلوند:

لدينا ملاحظة في غرفة Adobe Connect. وهو من عبد المنعم غليلا – أعتذر إن لم أنطق الاسم على النحو الصحيح. في الحقيقة ملاحظتين. الملاحظة الأولى مرتبطة بالمعطيات [في] الخرائط وما إذا كنتم تستطيعون أن تأخذوا بعين الاعتبار IDN TLDs؟ وملاحظته الثانية هي "أعتقد أنها خرائط ASCII وأعتقد أن هذه الخرائط هي لـ ASCII و IDN TLDs، لذا هل بإمكاننا التمييز بين ASCII و IDN DNSSEC لـ IDN TLDs الموقعة على الخارطة حتى يتضح الأمر أكثر؟"

جاك لاتور: أعتقد أننا نستطيع إحالة الاستفسار على دان يورك كي يجيب عليه. حسنا، الكثير من العمل هو عمل يدوي وهو مبني على تحيين المجتمع له بشأن الحالة. لذا في حال توصله بالمعلومات، فأنا على يقين من أنه يستطيع القيام بذلك. وأعتقد أن دان سيتطوع للقيام بذلك. نعم، أية أسئلة؟

شخص غير محدد: اسمي [بتعذر تمييز الصوت]. أنا من سجل .ID. وأرى أنه في تلك الخارطة من اندونيسيا. أنهم يسمون DS من خلال الجذر. ما هي طبيعة معايير DS؟

جاك لاتور: ما هي معايير DS في الجذر؟ هذا يعني أنك وقعت منطقتك مع DNSSEC، وأعطيت بعدها IANA سجل DS كي يتم وضعه في جذر المنطقة، لكن مسجلك يرغب في توقيع نطاقه، في حال وقع مسجلك على نطاقاته، فلا يمكنه وضع سجل DS الخاص به في منطقتك لكون أمين السجل لا يقبل بذلك الأمر. لذا لم تقم بـEPP لقبول DNSSEC أو واجهة الويب أو نظام ما للقيام بذلك.

شخص غير محدد: أتفهم، لا بأس. هل يمكنك تزويدنا ببعض روابط URL لقبول ذلك لبعض نطاقاتنا الفرعية أو TLD آخر؟

جاك لاتور: حسنا هل في السجل؟ كيفية القبول؟

شخص غير محدد: أجل، السجل. نحن ضمن سجل .ID.

جاك لاتور: هل كتبت السجل الخاص بك أم استخدمت سجل طرف ثالث؟

شخص غير محدد: الآن نستخدم جزئياً سجل طرف ثالث لكن نظرنا في DNSSEC وحالة النشر، فلا نشغل كلياً مع سجلنا. وفي الواقع الآن نستخدم سجل طرف ثالث.

جاك لاتور: لذا تحتاج لطلب دعمهم لـ DNSSEC.

شخص غير محدد: أجل، نحن بحاجة لتوفير بعض -

جاك لاتور: إذن أنتم بحاجة للعمل مع أمين سجلكم لإجبارهم على دعم ذلك.

شخص غير محدد: أجل، الآن نطلب من أمين السجل دعم DNSSEC. لكن ليس جميع أمناء السجل يدعمون كلياً DNSSEC.

جاك لاتور: إذن هل تدعمون EPP بـ DNSSEC؟

شخص غير محدد: نعم، صحيح.

جاك لاتور: إذن تقنيا، يتعين أن يكون الدعم تشغيليا. إذا كنت أمينا للسجل ولا تدعمون ذلك، فهذا أمر مختلف. في حال تدعمون مفاتيح DS أو DNS لـ EPP فيتعين أن يصبح اللون أخضرا.

شخص غير محدد: لدينا حتى الآن حوالي 15 أمينا للسجل، لكن قد يكون ذلك جزئيا، ربما سبعة أو ثمانية منهم حتى الآن هم من يدعمون كليا DNSSEC. لكن الباقي ليس كذلك –

جاك لاتور: ما هو TLD مرة أخرى؟

شخص غير محدد: .ID.

جاك لاتور: ID؟

شخص غير محدد: ممثل إندونيسيا.

جاك لاتور: ممثل إندونيسيا، حسنا. إذن أصبح لونكم أخضرا.

شخص غير محدد: كلا، ليس أخضرا. أنا الآن في منطقة ذات اللون الأخضر الفاتح. أجل. شكرا.

جاءك لاتور:

لذا يستحسن أن يكون لنا لون مختلف عندما يدعم جميع أمناء سجلكم DNSSEC مثل نجمة، لنضع نجمة هناك. هل رأيت؟ أقترح أن يتطوع دان ويضع النجمات. رائع. هل من أسئلة أخرى؟ هذه جلسة للتفاعل. كلما طرحتم أسئلة كلما توصلنا إلى حلول. حسناً. فرصة أخيرة. لا؟ شكرًا.

حسنًا لدينا الآن ورشة عمل أولى عبارة عن حلقة نقاش بشأن أنشطة DNSSEC. وأنا من سيدير النقاش. ثم لدينا مايكروفونات متجولة. والذي سيتحدث عن تنفيذ DNSSEC في أسماء النطاق السعودي. مرحبًا.

رائد الفايز:

مرحبًا بكم جميعًا. اسمي كاليب. أتمنى ألا يسبب تكرار الأمر إزعاجًا للكثير منكم. قمت بتقليص الشريحة بعض الشيء لتوفير بعض الوقت. أنا من SaudiNIC. قمنا مؤخرًا بنشر DNSSEC في العربية السعودية، كلا .saudia و TLDs و IDN. كان ذلك سنة 2016 و SA. في هذه السنة.

حسنًا، لا يظهر الخط العربي بشكل صحيح. أعتذر عن ذلك، لست متأكدًا لماذا. لكن على أي حال لنقم بتغيير اللغة إلى الإنجليزية. على أي، الحروف منفصلة، لا أعلم لماذا. ليس ذلك مشكلًا، لكن على أي ربما سأبعث لكم بنسخة محينة. شكرًا.

إذن بدأنا التعامل مع DNSSEC من خلال ثلاث مراحل. كانت منهجيتنا تقوم على الانتشار عبر ثلاث مراحل. المرحلة الأولى كانت مرحلة التتبع. وكنا نراقب RFCs والأدوات والبرمجيات، وكنا ننتظر بلوغها مرحلة النضج على أمل التمكن من الدخول دون خطأ أو تغيير جذري لاحقًا في المستقبل كونكم ترغبون في أن يكون نشر DNSSEC سلسًا في العربية السعودية. في سنة 2015، بدأنا العمل الأولي.

لذا بدأنا القيام بدراسة شاملة ولدينا العديد من الدول – قمنا بتحديد معيار مع العديد من الدول، الدول الرائدة في DNSSEC. قمنا بقراءة RFCs وتوصلنا إلى خارطة للنشر، لذا عرفنا كيفية التعامل مع هذا الأمر بتفصيل. والخطة في مرحلة التنفيذ. المرحلة الأولى كانت سنة 2016 والثانية هذه السنة، بداية هذه السنة، وأتمناها مسبقًا.

إذن منهاجيتنا كانت خطوة خطوة. لا نقوم بحرق المراحل أو بخطوات كبيرة. نركز أكثر ونتعلم بشأنها ونقرأ أكثر ونقوم باختبارات وقمنا بإنشاء مختبر تجارب وكل مصطلح نجده في DNSSEC RFCs نحاول قراءته ونشره واختباره والاستئناس به. وقد قمنا بالدراسة. وبعدما أجرينا الدراسة، توصلنا إلى أن عملية النشر ستتم عبر ثلاث مراحل. المرحلة الأولى، التوفر وبناء خبرات محلية في SaudiNIC وفي منظماتنا SITC و CERT وأيضا ولدى فاعلي الاتصالات.

المرحلة الثانية كانت بناء نموذج حتى نبدأ توقيع .saudia في IDN. كانت منطقة صغيرة جدا. قمنا بتوقيعها ومكنا عملاءنا من توقيع رموز DNS وحاولنا اختبارها والتأكد من فهمهم للمعلومات وبالتالي استطاعتهم نشرها بطريقة سليمة وأمنة في جميع نطاقاتهم وفي نطاقات عملائهم. قمنا بإعداد قائمة بريد داخلية، فريق داخلي يتضمن العديد من الأشخاص، وأي أمر نرغب في مناقشته نطلب فقط من الجميع الاطلاع عليه واتخاذ القرار، وأيضا تحديد المعايير لـ DNSSEC، ومعايير KSK و GSK الأمور التقنية التي نتوفر عليها في هذا المختبر. ثم نذهب بعدها للتشغيل ونقوم بفتحه لفائدة عملائنا قصد تحميل DNS الخاص بهم.

وقمنا بإجراء التدريب. كوننا نعتقد أن التدريب هو العامل الرئيسي لنجاح DNSSEC. لذا قمنا بإجراء تدريبين. التدريب الأول كانت مدته ثلاثة أيام. شارك فيه 25 شخصا من 11 هيئة حكومية بمعية الفاعلين في ICT. التدريب الثاني – كان ذلك في تشرين الأول (أكتوبر) 2015. التدريب الثاني كان في أيار (مايو) من هذه السنة. وازداد نسبيا عدد المشاركين إلى 41 شخصا من 29 هيئة حكومية والفاعلين في ICT وبعض البنوك أيضا. واستضفنا حدثا عاما طيلة يوم واحد في أيار (مايو) مباشرة بعد التدريب. وشهد مشاركة 120 شخصا من السعودية، أغلبهم كان رؤساء مصالح IT أو رؤساء مصالح الأمن و ISPs والعمليات. كان حدثا مفتوحا لكل مهتم بـ DNSSEC. وقمنا بجميع هذه الدورات التدريبية بالتنسيق مع RIPE و MENOG و ICANN.

وهذه بعض الصور من جلسات التدريب. صور الجهة اليمنى تخص التدريب الأول. وصور الجهة اليسرى تخص التدريب الثاني. كان ذلك حدثا عاما قمنا بتسليم الشواهد للمدربين قصد جعلهم فخورين بتوفيرهم على معرفة بخصوص DNSSEC. وهذه

بعض النتائج. إذن نتوفر على تصريح الممارسة SaudiNIC DNSSEC ونحن أول من أعده باللغتين العربية والانجليزية. وهو متوافق مع RFC 6841 وهذا هو التصريح بالممارسة DNSSEC. وقمنا كذلك بإعدادات DNSSEC.

قمنا بإعداد الكثير من الإجراءات تهم طريقة التعامل مع DNSSEC وكيفية القيام بحفل الافتتاح وكيفية تثبيت المفاتيح وكيفية إعداد تأمين جديد في حال تعرض أحد المواقع لخطر ما – العديد من الإجراءات. وقمنا بهذا التقييم لأجل DNSSEC حتى نعرف ما الذي ينبغي القيام به في حال تعامل بعض الأشخاص المهمين مع بعض كلمات السر أو صناديق لنموذج أمن الأجهزة أو قصد التوقيع وواجه مشكلا ما. ما الذي ينبغي القيام به أيضا؟ لدينا جدول تدبير المخاطر الذي يبين ما الذي يتعين القيام به بالضبط. قمنا بإعداد موقع الكتروني وأدوات وكلاهما متوفر بالعربية والانجليزية. وقمنا بالتشغيل الكلي.

وهذه أهم النتائج. هذه هي [DBS] التي حدثكم عنها. وهذه هي إعدادات DNSSEC الخاصة بنا في البنية التحتية. لذا تستطيعون رؤية في الجهة اليمنى في الأعلى هناك غرفة DNSSEC حيث نقوم بالأمر الرئيسية، الإنشاء الرئيسي والتثبيت الرئيسي والعديد من الأمور وهي آمنة لذا نقوم بتخزين HSM مع البطاقات داخل الخزانة بعد إنشائها. لا يمكن لأي أحد الدخول أو مغادرة الغرفة ما لم يكن هناك إجراء خاص بذلك. ولدينا غرفة دعم. لدينا موقعان، مركز البيانات 1 ومركز البيانات 2 لهما موقع ومحكم خفي وخوادم عامين.

إذن هذه مجموعة من الإجراءات التي قمنا بإعدادها. وقمنا بإطلاق تشغيل DNSSEC في saudia. كنموذج في 2016، حزيران (يونيو) 2016. وكنا أول بلد DCC يستخدم DNSSEC. ودعونا كما قلت لكم ISPs و DSPs ومزود خدمة البيانات للمشاركة في DNSSEC. الانطلاقة الرسمية للثنتين. Saudia. [غير مسموع] في السعودية والعربية كانت في حزيران (يونيو) من هذه السنة. وكنا أول من قام بفتح الخدمة في المنطقة لفائدة عملائنا. وقمنا بحفل إنشاء رئيسي. ووقعنا المناطق. ونشرنا DS [غير مسموع] لـ IANA. قمنا بتعيين جهاز التسجيل للشروع في قبول DS لفائدة عملائنا. قمنا بحملات توعية في الجرائد والانترنت وفي قوائم البريد. كما أنشأنا موقعا بالعربية. وهو www.DNSSEC.sa وهو متوفر بالعربية والانجليزية.

وهذا من خارطة نشر ISOC DNSSEC. يظهر أن SAs. هو بلون أخضر. أخضر. داكن. وحمدًا لله على ذلك. وهذه صور من حفل الإنشاء الرئيسي. وهذه هي الفرق وجميعها فرق تنفيذية في CITC. وهناك أيضا مدقق ورئيس مصلحة الأمن. ومعنا [CERT]. ومعنا بعض الخبراء من DNSSEC.

هذا هو الموقع الإلكتروني. وكما ترون هذه هي النسخة العربية. لأنكم تتوفرون على صور، يجب علينا أن نكتب ونبين للناس أن فهم DNSSEC أمر بسيط. لذا فالمعرفة متوفرة بلغتهم لأنه سيصعب عليهم القراءة والفهم بالانجليزية. لذا إن كان المستخدم لا يجيد جيدا الانجليزية، بإمكانه قراءة ذلك بالعربية. سيكون من السهل عليه/عليها فهم ذلك.

وهذه هي الأدوات. وهذا هو محقق سجل DS. لذا عندما تضع مفتاح DNS الخاص بك وسجل DS فستقوم الأداة بالتحقق من توافقهما من عدمه. أو تستطيع أن تضع اسم نطاقك وستقوم الأداة بجلب سجل مفتاح DNS من ملف منطقتك. وبعدها ستساعدك في إنشاء سجل DS المقابل.

وإلى غاية متم أيلول (سبتمبر)، لدينا أكثر من 50000 من أسماء النطاق. ولدينا 55 نطاقا مشغل DNSSEC إلى غاية الأمس أو اليوم قبله. 33 نطاقا تم تشغيله و DNSSEC مشغل في sa. وثمانية في saudia. و IDN، وستة في com.sa، ستة في net.sa، وواحد في org وواحد في gov. ونحن بحاجة للعمل أكثر في gov. وفي المجال البنكي، بمطالبتهم بنشر DNSSEC في أقرب وقت ممكن.

مرة أخرى، نحن بحاجة أكثر لحملات التوعية والتشجيع. فالأرقام جد متدنية لكن نأمل أن ترتفع في المستقبل. نحتاج إلى مراقبة أي تحسين في برتوكول DNS لذا يتعين علينا التركيز على 3, 5 NSEC والقضايا الجديدة للتحديث الآلي الرئيسي ومثل هذه الأمور. وهي أمور مهمة يتعين علينا مراعاتها. كما نحتاج إلى مراقبة مفتاح التبديل الخاص بنا. لذا لدينا KSK الخاص بنا لمدة سنة واحدة و ZSK لمدة ستة أشهر، وتتغير كل ستة أشهر. لذا يتعين علينا مراعاتها.

إذن تم استخلاص الدروس، والأمور التي أرجو من الجميع أن يركز عليها وخاصة الوافدين الجدد هي حاجتهم إلى بناء تجربة محلية. ويحتاجون إلى إنشاء مختبر للقيام

بالتجارب – ما الذي حدث؟ نعم، حسنًا. أجل [إطلاق من هذا المختبر] اختبار الجهاز، التطبيقات، مراقبة الأدوات لاختبار المعايير لفائدة DNSSEC. ومراقبة واختبار الأدوات لفائدة ملف المنطقة. أجل، تحتاجون إلى تطوير أدوات المراقبة والاختبار.

لذا لا تقومون فقط ببناء ونشر ملف منطقتكم. بل تحتاجون للتحقق منه قبلها ومراقبة إن كانت التوقعات ما تزال صالحة أم لا. قد تضعون بعض النطاقات المهمة للتركيز عليها حتى لا يتم نشر ملف المنطقة في حال وجود مشاكل في بعض أسماء النطاق. تحتاجون إلى تشغيل تلقائي. وبالتحديد عند حفل الإنشاء الرئيسي، فلا تتخلوا عن الإنسان لأن الإنسان يخطئ. تحتاجون إلى توفير أدوات الدعم، المواقع الإلكترونية لأن المستخدم قد يحصل له ارتباك.

أعتقد أن هذه هي الشريحة الأخيرة من عرضي. نعم، هذه هي. شكرًا جزيلاً لك.

شكرا لك، راند. هل لديكم أية أسئلة؟ لدي سؤال واحد. نعم.

جاك لاتور:

هذا أمر في غاية الأهمية، شكرا لك. ما هي العملية التي يستخدمها المسجلون لتحميل مفاتيح DS الخاصة بهم كي تتماشى مع نطاقاتهم؟

جون ليفين:

أجل. يستطيعون العودة إلى سجلنا ثم تحميل أسماء نطاقاتهم.

راند الفايز:

هل هناك أي API أم أن العملية يدوية كليا؟

جون ليفين:

كلا، كلا، هي تلقائية. لذا هناك نموذج. يتم ملء DS ثم القيام بالتحقق من ذلك.

راند الفايز:

جون ليفين: كيف أستطيع أن أطرح سؤالي جيدا؟ إن كنت مسجلا له 20 اسما، هل يتعين علي إدخال كل اسم على حدة في نموذج الويب؟

رائد الفايز: أجل، نعم.

جون ليفين: حسناً. حسناً. شكراً.

جاك لاتور: كان هذا سؤالي. هل من أسئلة أخرى؟ روس؟

روس موندي: ها نحن. شكراً. شكرا لك يا رائد على هذا العرض القيم. لقد قمت بعمل رائع هناك. وأعلم أن هذا تأكيد من DNSSEC لكن كان لدي فضول إن كان لديكم نفس إجراءات تدبير المخاطر والعودة إلى انسياب المحتوى الحقيقي للمنطقة عندما يزودكم المسجلون بمعلومات سجلاتهم DNS، سجلاتهم أ وما شابه ذلك. هل لديكم عمليات مقارنة وإجراءات وتأكيد على محتوى المنطقة بعينها؟ لأن هذا الأمر في الحقيقة هو ما تقوم به DNSSEC وهو الحفاظ وحماية والتحقق من محتوى المنطقة. لذا ينتابني فضول عما إذا قمت بالنظر في مجموعة من الأنشطة لمحتوى المنطقة.

رائد الفايز: أولاً وقبل كل شيء، إذا أراد شخص تحميل تفويض سجل الدخول DS الخاص به، فإن نظامنا يتحقق و يتأكد من أن DS مطابق لمفتاح نظام اسم النطاق DNS. و حالياً، هذا هو الاختبار الوحيد الذي نقوم به، وسنرسل له تحذيراً، وإذا أراد تجاهله فسيكون له - سنعرض له رسالة تحذير. و يمكن أن يحتوي هذا منطقتك الوهمية وربما لن يستطيع الناس الوصول إلى اسم نطاقك. ولكن ربما مستقبلاً، يمكن أن يكون لدينا بعض الإعدادات

التي ترصد ملفات المنطقة، وترى هل التوافق صالحة أم لا. ولكن في الوقت الراهن، لم نعلم بأي شيء. ولكن نأمل أنها ضمن الخطة. أمل أن أكون قد أجبت على أسئلتكم.

تقريبا و لكن علينا المتابعة. أريد أن أسأل أكثر في وقت لاحق. جولي؟

روس موندي:

حسنا لدينا سؤال في الدردشة ولدينا تعليق كذلك. السؤال، مررت عليه. السؤال من زينب الفارسي. ما هي التحديات الرئيسية التي واجهتكم؟

جولي هيدلوند:

في الواقع، تتمثل التحديات الرئيسية في بناء فريق متخصص في الامتدادات الأمنية لنظام اسم النطاق DNSSEC. فقد مثل هذا العائق الأساسي بالنسبة لنا لأن الإعداد كان موجودا. كان كل شيء جاهزا لكننا كنا بحاجة لقراءة طلبات تقديم التعقيبات RFCs، وفهم ما يجري وراء كواليسه. إن الأشياء التي تحتاجها إذا كنت ترغب في بناءه، هي فريق بإمكانه أن يفهم ويستوعب الأوقات المختلفة، و المعلمات المختلفة لـ DNSSEC لأنها مرتبطة ببعضها البعض.

رائد الفايز:

و نقضي تقريبا مدة أربعة أشهر فقط لمعرفة ما إذا قمت بزيادة فترة بقاء البيانات فعالة و TTL، ثم أن مفتاح التوقيع له علاقة بذلك، وهذه المعلمات لها علاقة بالثالثة. لذا سيكون سهلا علينا إذا قام أحد فعلا ببناء علاقة على شكل صيغة بين معلمات DNSSEC. فإذا قمت بوضع 3 TLZ، فسيضطر هذا إلى مضاعفة أرضية TTL. سيكون ذلك مشكلا أو شيئا من هذا القبيل. فإذا وجدت صيغة المعلمة، سيكون ذلك أفضل. لقد قمنا الآن بتوثيقها و نخطط للقيام بشيء لمساعدة الآخرين ولكن لم نعلم بأي شيء. بالإضافة إلى الخبرة المحلية، فبناء الخبرة المحلية كان تحديا رئيسيا بالنسبة لنا.

جولي هيدلوندا: لدينا تعليق واحد. التعليق من عبد المنعم جليلا. شكرا جزيلًا، رائد للحفاظ على الهوية العربية باستخدام اللغة العربية في عرضك التقديمي. تنفيذ خطة توعية جيدة باستخدام لغتك المحلية.

جاك لاتور: حسنًا. شكرًا. المتحدث المقبل هو كادر أردوغان من تركيا. وستحدث عن أنشطة DNSSEC في تركيا.

كادر أردوغان: طاب صباحكم. أنا في انتظار الشرائح. أجل. هناك مشكلة فيها ولكن على أي حال، نعم، حسنًا. هذا هو كادر أردوغان من tr. ccTLD. أنا هو المدير الفني. لا يعمل؟ حسنًا. أنا من تركيا وسأقدم لكم عرضًا قصيرًا حول أنشطة DNSSEC في تركيا. كما ترون، بلد ملون جدًا. يجب عليكم زيارته إذا لم تزوروه بعد. عفوًا؟ حسنًا.

تركيا قد تكون واحدة من أكثر البلدان وعيا بـ DNS في العالم. هل هناك أي شخص لا يعرف 8.8.8.8؟ نعم، إذا كنتم تستطيعون رؤية هذا، فيمكنكم أن تجدوا هذه التشكيلة في [غير مسموع] شقة في تركيا. تم التقاط هذه الصورة قبل بضع سنوات بينما كانت الحكومة تبحث في وسائل الاتصال الاجتماعي عن طريق تصفية DNS. فتعلم الجميع في البلد كيفية تشكيل DNS الخاص بهم. أعرف أن هذا عرض تقديمي لـ DNSSEC. ولكن في تركيا، لا يوجد حاليًا أي مزود خدمة إنترنت ISP يصادق على DNSSEC. لذا فإن DNS الخاصة بغوغل مهمة. ومن خلال تصفية حكومة DNS [غير مسموع]، يعرف الأشخاص DNS الخاصة بغوغل.

جاك لاتور: غوغل يصادق على ذلك؟

كادر أردوغان:

أجل. تاريخ قصير عن ccTLD، nic.tr. في سنة 1991، تم تأسيس أول اتصال بالإنترنت من جامعة الشرق الأوسط التقنية. وفي سنة 1995، تم تحويل.tr. و في 1998، أنشأنا مجموعة عمل DNS. وهو في الواقع أول نموذج حكومة أصحاب المصلحة المتعددين. فجميع الأطراف تقرر كيفية تنظيم.tr. في سنة 2003، أنشأنا تطبيق شبكة، تطبيقات آلية بالكامل، والمدفوعات، معالجة الوثائق، الخ.

في سنة 2006، قمنا بتنفيذ اسم النطاق المدوّل IDN. لدينا ستة أحرف، والتي ليست في نظام الترميز المعياري الأمريكي لتبادل المعلومات ASCII. لقد كان سهلا بالنسبة لنا. فهي ليست مثل اللغة العربية. في سنة 2008، قمنا بتنفيذ نظام التسجيل /أمين السجل. وهي ليست بروتوكول التزويد المرن EPP. فهي [استنادا لذلك] APA. وفي سنة 2010، نشرت الحكومة لائحة داخلية ، لدينا صراع بين الوزارة، وزارة النقل والاتصالات. نحن نتفاوض، و ما زلنا نتفاوض.

حول DNSSEC في تركيا، لا أحد يعرف ذلك في الواقع. لا أحد يهتم بها. وسيكون أمرا مبتذلا ولكننا لسنا مجرد نكرة. نحن نعمل بجد. ونعمل بنشاط. الوضع الحالي، .tr. لم توقع بعد للأسف. لا أحد من المشغلين الكبار يريد المصادقة. و ليس فقط مشغل كبير واحد. فعلى ما أعتقد، لا أحد من المشغلين. وبسبب ذلك، ليس لدينا مشكلة في استبدال مفتاح توقيع شفرة الدخول الأساسية KSK بتركيا. ربما يجب أن أرجعها في - نعم. وصناع القرار ليسوا على علم بـ DNSSEC.

هناك بعض الأشياء الجيدة. ونحن حريصون على التوقيع بصفتنا ccTLD. المجتمع التقني يتحدث عنه. و نحصل على بعض الطلبات من مالكي النطاقات لتسجيل أسماء النطاقات الخاصة بهم. إنه جيد. كما ننظم بعض التدريبات وورش العمل في البلاد. و ما قمنا به إلى الآن، التدريب الأول سنة 2014. لقد استضفنا التدريب. وقمنا بتنظيم التدريب بمساعدة مؤسسة الإنترنت للأسماء و الأرقام المُخصصة ICANN و NSRC. وكان على الصعيد الوطني. كان الفريق الفني لـ.tr. كلهم متدربين. و أما بالنسبة للمدربين فقد كان ريك لامب من ICANN وفيل ريجنولد من NSRC.

قمنا كذلك بتنظيم تدريب آخر لـ DNSSEC في آذار (مارس) سنة 2006، في اسطنبول. وكان ذلك على الصعيد الدولي. قمنا بتنظيمه مع الشبكات الأوروبية لبروتوكول الإنترنت RIPE في MENOG 16. مرة أخرى، كنت أنا من nic.tr وريك لامب من ICANN المدربين. وكان هناك تدريب آخر سنة 2006. وكان على الصعيد الوطني. و تكون هذه التدريبات على مدة خمسة أيام من التدريبات التقنية جدا، والمعقدة للغاية. ليس من السهل تنظيمها. ليس من السهل العثور على أشخاص للتدريب لأن DNSSEC هو - في الواقع DNS هو موضوع ضيق. و DNSSEC أضيق من الضيق. لذلك ليس من السهل العثور على الأشخاص المناسبين.

قمنا بتنظيم ورشة عمل أخرى في 2017 في منتدى DNS تركيا. كانت تلك الثالثة في الواقع. وكانت ورشة عمل لمدة نصف يوم. و هذه صور منها. أجل. و هذا ريك يدرسنا. من درسناهم. حتى الآن، قمنا بتدريس أزيد من 50 تقنيين، والذين هم في الغالب مسؤولون عن DNS في منظماتهم. 20 منهم من الوزارات الحكومية والهيئات التنظيمية والجيش. 10 منهم من الجامعات، و 10 من أمناء السجلات، و 10 من مشغلي الشبكات. ومرة أخرى، كما قلت، من الصعب حقا تحديدهم. ولكن لدينا لجنة جيدة الآن. عذراً.

علينا أن ننظم المزيد من التدريبات لأننا درسنا خيرا بأن DNSSEC هي قابلة يدوية. و لا تعرف متى ستفجر. و لذلك نحن بحاجة إلى المزيد من الخبراء. نحن بحاجة إلى ورش عمل. ونحن بحاجة إلى الثروة. قلت الثروة لأنه علينا جعل الرئيس الكبير صديقا لـ DNSSEC. إذا كنت تتحدث تقنيا، فإنهم لا يعرفون شيئا عن ذلك. إنهم لا يفهمون ذلك. لذا أعتقد أن الثروة هي الكلمة الصحيحة.

ما هو التالي؟ توقيعها. شكرا لكم على أي حال. بالمناسبة هذا هو صوتي. وهذا كل شيء.

شكراً. هذا جيد جدا. هذه هي المرة الأولى التي نحصل على واحدة من هذه. هل هناك أسئلة لكادر؟ نعم، كريستيان؟

جاك لاتور:

كريستيان: أنا مع .nl للتسجيل بهولندا. أين تعتقد أن DNSSEC من المفترض أن تبدأ في تركيا هل مع مزودي خدمات الإنترنت ISP من حيث المصادقة أو مع السجل من حيث التوقيع؟

كادر أردوغان: في الواقع، إنها ليست فقط معنا مع ccTLD. يجب أن نوقع عليه أولاً. ثم ISP كما أعتقد.

كريستيان: لأننا نتبع نفس النموذج في هولندا. لذلك في البداية عندما بدأنا في التوقيع، لم يكن هناك شيء سوا فيما يخص المصادقة ونحن فقط - يعني أنه عليك كسر هذا التعادل في موضع ما وقد بدأنا من جانب التسجيل.

كادر أردوغان: أجل.

جاك لاتور: هل هناك أسئلة؟ جيف.

جيف هوستون: لاحظت خلال السنة الماضية والنصف ، أن استخدام DNS العام لغوغل قد انخفض بالفعل من حوالي 23% من المستخدمين في تركيا إلى حوالي 7% تقريبا. هل هذا بسبب أنهم أوقفوا غوغل أو أن ISP يضعون اعتراضات في DNS ؟

كادر أردوغان: أنا لا أعرف الإجابة الصحيحة على هذا. ولكن أستطيع أن أقول تخميناتي. أعتقد أن الحكومة تعترض الأمور، وأنا لا أعرف في أي مرحلة بالضبط.

جيف هوستون: هل هذا يدفع إلى الاهتمام بأشكال التشفير والمراوغة في خصوصية DNS و الذي يمنع اعتراض تلك الدرجة الأولى؟ هل هناك اهتمام بهذه التكنولوجيا للتغلب على مشكلة الاعتراض القسري؟

كادر أردوغان: أنا لا أعرف ما الذي تغير.

جاك لاتور: هل هناك أسئلة؟ حسناً، شكرًا. المتحدث التالي هو راجيف كومار من NIXI. بخصوص تحديث تسجيل .in DNSSEC.

راجيف كومار: صباح الخير للجميع. مرحبًا؟ طاب صباحكم. أنا راجيف كومار من تسجيل nixi.in. محلل النظام في السجل [غير مسموع]. إنها فرصة جيدة لتعطيني - مرحبا؟ ستكون فرصة جيدة لتحديث تحديثات تسجيل .in، وتحديث DNSSEC. وجدول الأعمال هو تسجيل .in DNSSEC. ومشاركة المسجل، جهود السجل، موارد للمسجلين، مصادقات DNSSEC، والحالة الراهنة.

يعد تسجيل .in أول المعتمدين لـ DNSSEC. وتم توقيع منطقة .in سنة 2010. و تجري برنامج DNSSEC للأصدقاء والأسرة. في هذا البرنامج، يمكننا السماح لأعلى ISP وأمناء السجل لاختبار بيئتهم، والتعامل مع البيئة. وإذا كان هناك أي خلل، ترجع لنا ونقوم نحن بكل شيء.

وبعد سنة واحدة، في 2011، تم تقديم DNSSEC في بيئة الاختبار. لذلك نبدأ DNS بيئة الاختبار لأمناء السجل. ثم أمناء السجل المختبر يختبرون بيئتهم ويسمحون للمسجل بالتوقيع على سجل DS. بعد شهر واحد في 2011 تشرين الثاني (نوفمبر)، كنا نستقبل سجل DNS.

مشاركة أمناء السجل، لدينا 121 أمين سجل معتمد في جميع أنحاء العالم. ومن بينهم 39 DNSSEC ممكن بما في ذلك أول 10 أمناء سجل in. في DNSSEC المتقدمة. وتوفر خدمات DNS لمسجليها. نحن 2 مليون اسم نطاق مسجل [غير مسموع]. ومن أصل ذلك، تم التوقيع على 1287 حتى أيلول (سبتمبر). وهي نسبة أقل من 1٪. ولكننا نحاول بالقيام بأفضل ما [عندي].

ونبلغ بأننا نجري جلسة لأمناء السجل لتشجيعهم على ترويج DNSSEC. و نجري كل عام اجتماعا وجها لوجه مع أمناء السجل [غير مسموع] ونقدم عرضا إيضاحيا. فضلا عن أننا ننظم تدريبا عمليا، ورشة عمل، و برنامج التوعية للمجتمع التقني مثل ISP [حكومة] الهند وأمناء السجل بمساعدة ICAN، و مركز معلومات شبكات آسيا والمحيط الهادئ APNIC. و خلال كل عام، نقوم بإجراء SANOG. إنها مجموعة منظمة شبكة جنوب آسيا حيث ننظم التدريب العملي لـ DNS لمدة خمسة أيام.

موارد [أمناء السجل] للمستوى متواجدة على موقعنا على الانترنت، وإضافات EPP RTK متاحة على موقع السجل. قم بتحديث عميل بروتوكول التزويد المرن EPP لدعم تحكم DNSSEC OT&E. DNSSEC البيئية متاحة أيضا على موقعنا.

أما بالنسبة لجزء المصادقة، ففي حالة الهند يمكننا الحصول على باحثين فرديين. ويعطيني حالة 447 اسم خادم، محلل مفتوح. 34 فقط من خادم الأسماء مصادق عليها من 144. DNSSEC اسم الخادم على علم بـ DNSSEC ولكن لم تتم مصادقتها حتى الآن. 299 اسم خادم لا يدعم DNSSEC. هذه هي حالة المصادقة في الهند، جزء المصادقة. كما أننا ندعم اسم النطاق المدوّل IDN في توقيع DNSSEC. و [غير مسموع] موقعة ومن الأفضل لنا أن يبدأ IDN بتوقيع اسم النطاق المشترك. شكراً. أي سؤال؟

شكراً. هل لديكم أية أسئلة؟ روس؟

جاك لاتور:

روس موندي: شكرًا لكم على هذا العرض التقديمي. أنا أتساءل إذا كان بإمكاننا العودة إلى شريحة

المصادقة، أعتقد أنها كانت قبل هذه. كيف عرفت عدد المحللين المصادق عليهم؟

راجيف كومار: في الواقع، هناك في الجامعة، وجامعة أمريتا يجرون ويقيمون المجتمع الهندي وربما

هناك إعداد يوفر لي حالة أجزاء DNS المصادق عليها وكل ذلك.

جاك لاتور: لذلك هل تعتقد أن هناك حلاً أكثر انفتاحاً في الهند من ذلك؟

راجيف كومار: أجل.

جاك لاتور: أكثر بكثير؟

راجيف كومار: ربما. هذا هو الموضوع. وسأتأكد من جامعة أمريتا وأعود إليكم لأنهم يوفر لي الحالة

التي تخص ذلك.

جاك لاتور: شكرًا. هل من أسئلة أخرى؟ ثلاثة اثنان واحد. حسنًا، شكرًا.

راجيف كومار: شكرًا.

روس موندي: أعتقد أن هناك سؤالاً عبر الإنترنت.

جاك لاتور: عذراً.

جولي هيدلوند: سيكون هناك سؤال في الدردشة على الرغم من انه ليس جاهزا بعد. ولكنني أردت فقط أن أشير أيضا إلى أن عبد المنعم جليلا غير قادر على أن يكون هنا ولكنه قام بتسجيل عرضه، والتحدث من خلال عرضه عبر مقطع صوتي. لذلك سنتابع ونبدأ عرضه مع مقطع الصوت، حتى وإن لم يكن هنا. و افتراضيا، سيظهر في وقت لاحق للأسئلة و الأجوبة، لديه مشكلة فقط في الوقت الراهن.

راجيف كومار: ثانية واحدة لأنني لا أفهم السؤال.

عبد المنعم جليلا: ... نائب مدير .masr ccTLD. كما أنني عضو في ICANN و عضو اسم النطاقات العالمية العربية. [غير مسموع] تعني باللغة العربية [غير مسموع]. وسيكون عرضي حول التحديات التي واجهتنا أثناء نشر DNSSEC. في الواقع سأذكر التحديات قبل وبعد النشر، وسأتحدث قليلا عن البرمجة النصية لنظام أسماء النطاقات DNSSEC. كنا نوقع أو نقبل .masr [غير مسموع]. الشريحة التالية.

لقد نشرنا DNSSEC لـ .masr ccTLD سنة 2015. و قبل ستة أشهر من نشر DNSSEC، لم تكن لدينا فكرة حول DNSSEC. يجب أن نعرف على الأقل ما هو DNSSEC وكيف يعمل. لقد سمعنا كلمة DNSSEC في قمة أفريقيا للإنترنت لعام 2014 في جيبوتي. و من هناك، بدأنا التفكير في كلمة DNSSEC. و أردنا معرفة بعض المعلومات حول DNSSEC وحصلنا على ذلك من خلال حضور ورش عمل DNSSEC. كانت لدينا بيتتان لهذا النظام الشامل للسجل.

البيئة الأولى هي إنتاج واحد. والثانية، استخدمناها للاختبار، وهي مطابقة تماما لإنتاج واحد مع قاعدة بيانات السجل، 3 خادم DNS WHOIS. وما زلنا نريد الحصول على

معلومات معينة حول كيفية عمل DNSSEC لذلك كان علينا إنشاء خادم جذر وهمي و المحلل بـ DNSSEC مصادق في بيئة الاختبار الخاصة بنا. لقد فعلنا ذلك، وحصلنا على المعلومات المطلوبة لبدء نشر DNSSEC في بيئة الإنتاج الخاصة بنا.

في بيئة الاختبار الخاصة بنا، وقمنا على منطقة masr. و كان كل شيء يعمل بشكل جيد. ولكن نسخة من برنامج التسجيل الخاص بنا كان يظهر في كل نسخة بغض النظر عن إضافة إشارة خاصية DS لنطاقات masr الفرعية من خلال واجهة السجل. بالمناسبة، نحن نستخدم برنامج السجل CoCCA. لذلك قمنا بتحديث نظام السجل وكان يعمل بشكل جيد. و قد تأخر واحد من اختبارات خادم DNS لمدة 10 دقائق. لذلك يجب علينا جعل نظامنا متزامنا في الوقت لذلك قمنا ببناء خادم الوقت وجعل كل خادم عميلا لزنابنا.

أردنا تأمين الاتصال بين السيد و العبد خادم DNS لذلك استخدمنا توقيع معاملات TSEC لمعالجة هذه المسألة في بيئة الاختبار الخاصة بنا. و حاولنا أن نكون على معرفة تامة باستكشاف أخطاء DNSSEC قبل أن نتجه في خط مع DNSSEC. و بعد نجاح الاختبار، أردنا تكرار ما فعلناه في بيئة الاختبار لبيئة الإنتاج الخاصة بنا. واستغرقنا أقل من 15 دقيقة لإعادة تكوين بيئة الإنتاج لنشر DNSSEC و TSEC.

ترتبط معظم مشاكل DNSSEC بجدران الحماية. لذا يرجى التأكد من إشراك مديري الأمان والشبكة حتى يتمكنوا من إجراء التغييرات المطلوبة قبل أخذ DNSSEC إلى الإنتاج. هناك نوعان من مشاكل جدار الحماية الأكثر شيوعا. الأول يشمل TCP، بروتوكول التحكم في الإرسال. هناك سوء فهم بين بائعي جدار الحماية ومسؤولي الأمن التي تقوم بحذف بروتوكول البيانات الميدانية للمستخدم - آسف، واستفسارات DNS تستخدم UDP و منطقة النقل تستخدم TCP. لسوء الحظ، هذا الافتراض ليس صحيحا تماما. تحاول استفسارات DNS أولا UDP ولكن تعود إلى TCP. إذا لم يتم تلقي أي استجابة من الاستفسار الأولي لـ UDP. أو إذا سربت الاستجابة معلومات مهمة بسبب اقتطاعها، فإن إمكانية وجود شيء ما في الماضي والرد على الاستعلام الأولي أعلى بكثير مع DNSSEC بسبب زيادة حجم الردود. و حتى تعمل DNSSEC بشكل

صحيح، فمن الضروري أن تفتح جدار الحماية الخاص بك. و من الضروري أن تفتح جدار الحماية الخاص بك لكل من TCP و UDP عبر المنفذ 53.

و ترتبط المشكلة الثانية بالحجم الجزئي لبروتوكول الإنترنت الاحتياطي IP. أدرك المصدر القديم لمعيار DNSSEC أن هناك مشكلة محتملة قد تتواجد مع استفسارات TCP. إذ تفرض آلات TCP عبئا أكبر على خادم DNS. كما أن TCP أكثر تكلفة من UDP بالنسبة للمعالجة. و لتجنب الكثير من حركة مرور TCP، فإن [غير مسموح] ملحق آليات توسيع نظام اسم النطاق (0) EDNS إلزامي لـ EDNS. DNSSEC. (0) هي واحدة من آلية التمديد لـ DNS. و معيار من بين أمور أخرى يسمح للعميل بالإشارة إلى أنه قادر على تلقي ردود DNS على UDP التي تكون أكبر من الحد السابق البالغ 512 بايت.

بعض جدران الحماية ليست على علم بأن معيار (0) EDNS يسمح بالحزم الأكبر و الأسهل لمنع حزمة EDNS باستخدام (0) EDNS أو منع أي حزمة DNS أكبر من 512 بايت بغض النظر عن إشارات (0) EDNS. جدران الحماية الأخرى تسمح للحزم الأكبر بشكل افتراضي في حين أن عددا قليلا من البائعين يطلبون تكوين جدار الحماية يدويا للقيام بذلك. يتم تعريفه في الحافلة التي تحمل الحزمة بأنه يجب التأكد من أن طبقة التطبيق على علم بمعايير (0) EDNS لتكون قادرة على اتخاذ القرار الصحيح حول إعادة توجيه الحزمة أو لا. لا يكفي اختبار أنك تتبع جدار الحماية الخاص بك الذي يسمح بالردود الكبيرة الواردة من DNS عن طريق إرسال استعلامات DNS إلى الإنترنت.

إذ يجب عليك أيضا اختبار بأن مصدرا خارجيا يمكن أن يتلقى ردود DNS أكبر التي يرسلها خادم DNS الخاص بك. إحدى طرق القيام بذلك هي استخدام محلل DNSSEC مفتوح. لذلك عليك اختبار وتكوين جدار الحماية الخاص بك للسماح باستخدام (0) EDNS وحزم DNS أكبر من 512 بايت على UDP. وأخيرا، نطلب من جهة الاتصال الإدارية masr. تقديم سجل DS إلى ICANN للتحقق من الشفرة وإضافة منطقة داخل منطقة الجذر.

الشريحة التالية. بعد نشر DNSSEC، أظهرنا معرفة كيفية الحفاظ على نظامنا متصلًا في كل وقت بدون انقضاء التوقيع. لذلك وضعنا نصًا لإقالة المنطقة بعد ولادة منطقة جديدة من نظام السجل مع القدرة على النظر في أخطاء للمسؤول. كما يقدم DNSSEC مهام تشغيلية جديدة مثل مفاتيح متجددة، وإقالة المنطقة. ويجب أن تنظم هذه المهام على شكل فترات دورية. لم نقم بأي استبدال للمفاتيح إلى الآن. ولكننا سنقوم بذلك خلال هذه السنة.

مرة أخرى، ينبغي أن نكون [غير مسموع] جدار حامي لـ DNSSEC. انتبهوا، ترتبط معظم مشكلات DNSSEC بجدران الحماية. لذلك عليكم أن تتأكدوا مرة أخرى من إشراك الأمن الخاص بكم ومسؤول الشبكات. وتتمثل مهمتنا الآن في نشر DNSSEC بين أمناء السجلات المحليين الأربعة. الشريحة التالية.

كما لاحظنا أن أحد DNS لا يستجيب لاستعلامات CB. وقد وجدت [MQ] الأكثر شيوعًا في جوهر الإنترنت حوالي 1500 بايت. وحتى هذا الحد يتم تجاوزه بشكل روتيني من خلال الردود التي تم توقيعها من قبل DNSSEC وقد يقوم بتوصيل العناصر المقصورة على هذا الحجم من [MQ] الذي يحاكي هذا الرد الموقع الذي سيتم إسقاطه. لذلك و لتجنب ذلك، وقعنا على المنطقة مع ZSK فقط. وحتى هذه اللحظة، لا يتوفر معظم محلي ISP على تمكين مصادقة DNSSEC. كما أنها ليست سوى سطر واحد من التشكيلة. الشريحة التالية. الشريحة التالية.

معظم أمناء السجل لدينا هم ISP. ويعتقدون أنه من الصعب توقيع نطاقاتهم وليس [غير مسموع] للقيام بذلك. ولديهم أيضا فكرة أخرى بأن نظامهم مستقر فلماذا عليهم تغيير نظامهم الحالي. الشريحة التالية.

لديهم هجمات ولكن يمكنهم التخفيف من ذلك. ليس لدى المسجلين فكرة عن DNSSEC. كما أن المكاسب الأمنية ستكون أفضل. سيتم حظر النطاقات ذات التوقيعات غير الصالحة. لديهم هجمات ولكن يمكنهم التخفيف من ذلك. ليس لدى المسجلين فكرة عن DNSSEC. وليس لدى واجهة أمناء السجل القدرة على إرسال سجلات DS إلى نظام

التسجيل من خلال ABB. لا يوجد عدد كاف من الموظفين لمراقبة واستكشاف مشاكل DNSSEC. الشريحة التالية.

الآن أريد أن أريكم بنية توقيع masr. والنص الآلي للإقالة. هذا النص كان في الأصل من قبل CoCCA للتعامل فقط مع ملفات المنطقة التي تم إنشاؤها حديثًا وتحريرها من قبل فريق masr. للتعامل أيضًا مع توقيع DNSSEC. الشريحة التالية.

بدأ النص ببعض المتغيرات التمهيدية مثل مدير ملفات المنطقة من السجل، مدير -

جاك لاتور: وهذا ما أردت توضيحه. شكرًا. هل لديكم أية أسئلة؟ حسنًا. نحن تمامًا مع الوقت المحدد للاستراحة. سنراكم بعد 15 دقيقة.

جولي هيدلوند: أنا أعلم أن عبد المنعم كان سيحاول أن يأتي للأسئلة والأجوبة ولكن أنا لا أعرف ما إذا كان هنا، إذا ما وصل. نعم، ها هو. لذلك إذا كانت لدينا أية أسئلة -

عبد المنعم جليلا: بدأ نصنا ببعض من النص التمهيدي مثل مدير ملفات المنطقة التي تم إنشاؤها حديثًا. و سيكون المدير مع المنطقة الموقعة. ثم تطبيق بعض التحقيقات لملفات المنطقة التي تم إنشاؤها حديثًا لمعرفة ما إذا تم إنشاء هذه المنطقة من أجل تطبيق بعض DNSSEC أولاً أم لا. ثم بعد ذلك، نقوم بفك ضغط سجلات ملف المنطقة التي تم إنشاؤها تلقائياً. ويتم إنشاؤه في الملف من السجل.

إذا كان لديكم العديد من المناطق التي تريدون توليدها، تريدون أن يوقع عليها DNSSEC باستخدام النص الخاص بنا، فهو مقبول. فقط القوا نظرة على المناطق. ثم نوقع على المناطق وبعد ذلك، نستخدم إعادة تحميل rndc. و ربما كنتم ترغبون في إعادة تشغيل برنامج الشراء الخاص بك. ولكن لا أوصي بذلك إذا كان لديكم العديد من

أسماء النطاقات مثل السجلات الأخرى ولكن لديكم فقط حوالي 800 اسم نطاق، أسماء نطاقات IDN. الشريحة التالية.

هذه لقطة من نصنا التلقائي، أولاً سيكون تمهيد المتغيرات. ثانياً سنتحقق من ما إذا كان ملف المنطقة، إذا قمتم بتغييره عن السابق أو لا. و بعد ذلك، فك ضغط ملف المنطقة، و بعد ذلك سأنظر إلى المناطق إذا كان لدي مناطق متعددة لـ DNSSEC للتوقيع عليه. بعد ذلك، يمكنني استخدام إعادة تحميل rndc. وهذا كل ما عندي. شكرًا.

شكرًا. هل لديكم أية أسئلة؟

جاك لاتور:

شكرا لك عبد المنعم على هذين الشطرين من العرض. واحد عن بعد و الثاني بحضورك الشخصي. ولدي سؤال. هل تقبل الموظفين الذين يقبلون سجلات DS لعملائك؟ وهل قمت بأية إعدادات للمصادقة على DNS الخاصة بهم أم لا؟

شخص غير محدد:

من اليوم الأول ونحن نقبل سجلات DS من أمناء السجلات لدينا. ولكن إلى الآن مشكلتنا هي أن أمناء السجل الخاص بنا ليسوا على علم بما فيه الكفاية حول DNSSEC. ونفس الشيء لعملائنا، سجلنا و ليس أمناء السجل. لذلك لا نقبل سوى سجل DS من أمناء السجل الخاص بنا. ليس لدينا سوى ثمانية أسماء نطاقات فقط، تم توقيع DNSSEC فقط.

عبد المنعم جليلا:

شكرًا.

شخص غير محدد:

جاءك لاتور: هل من أسئلة أخرى؟ حسنًا. و الآن نحن رسميا في استراحة. نعود بعد 15 دقيقة. أو لا، مع 10:30.

[نهاية النص المدون]