الدليل السريع:
استعد بأنظمتك لتبديل مفتاح الدخول الرئيسي KSK للجذر

ما المقصود باستبدال مفتاح الدخول الرئيسي KSK للجذر؟

تخطط مؤسسة الإنترنت للأسماء والأرقام المُخصصة (ICANN) لنقل، أو تغيير الزوج "الأعلى" لمفاتيح التشفير المستخدمة في بروتوكول الامتدادات الأمنية لنظام اسم النطاق (DNSSEC)، المعروف عادة باسم مفتاح الدخول الرئيسي (KSK) لمنطقة الجذر. وسوف تكون هذه هي المرة الأولى التي يتم فيها تغيير KSK منذ إنشائه للمرة الأولى في 2010. وهو يعتبر خطوة أمن هامة، بنفس الطريقة التي يُعتبر من خلالها تغيير كلمات السر بانتظام ممارسة حذرة من طرف أي مستخدم للإنترنت.

ينطوي تغيير المفتاح على إنشاء زوج مفاتيح تشفير جديد وتوزيع المكون العام الجديد على محللات تدقيق صحة الامتدادات الأمنية لنظام اسم النطاق DNSSEC. وحيث أن كل استعلام إنترنت باستخدام الامتدادات الأمنية لنظام اسم النطاق DNSSEC يعتمد على مفتاح الدخول الرئيسي KSK لمنطقة الجذر لتدقيق صحة الوجهة، فإن هذا سيكون تغييرًا كبيرًا. بمجرد إنشاء المفاتيح الجديدة، سيحتاج المشغلون مثل مزودي خدمة الإنترنت إلى تحديث أنظمتهم بالمفتاح الجديد بحيث عندما يحاول أحد المستخدمين زيارة موقع ويب، يمكنه تدقيق صحته مقابل مفتاح الدخول الرئيسي KSK الجديد.

لماذا تحتاج إلى الاستعداد

يستخدم حاليًا حوالي ربع مستخدمي الإنترنت حول العالم استبدالات تدقيق صحة الامتدادات الأمنية لنظام اسم النطاق DNSSEC التي قد تتأثر باستبدال مفتاح الدخول الرئيسي KSK. إذا لم يكن لدى هذه المحللات لتدقيق الصحة المفتاح الجديد عندما يتم تغيير مفتاح الدخول الرئيسي KSK، فإن المستخدمين النهائيين المعتمدين على تلك المحللات سيواجهون أخطاء ولن يستطيعوا الوصول إلى الإنترنت.

إذا لم تستخدم الامتدادات الأمنية لنظام اسم النطاق DNSSEC، فلن يتأثر نظامك بالاستبدال. ومع ذلك، ينبغي أن تعرف أن الامتدادات الأمنية لنظام اسم النطاق جزء هام لمنع سرقة اسم النطاق.

تقدم ICANN منصة اختبار للمشغلين أو لأي من الأطراف المعنية لتأكيد أن أنظمتهم تتعامل مع عملية التحديث الآلي بالطريقة الصحيحة. تحقق للتأكد من أن أنظمتك جاهزة عن طريق زيارة: **https://go.icann.org/KSKtest**.

إذا قمت بتمكين تدقيق صحة الامتدادات الأمنية لنظام اسم النطاق DNSSEC، فعليك تحديث أنظمتك باستخدام مفتاح الدخول الرئيسي KSK الجديد للمساعدة في ضمان وصول الإنترنت بدون مشكلات للمستخدمين.

2018 آذار (مارس) | Designed by ICANN Communications

ما الذي تحتاج إلى القيام به

يمكن تحديث أنظمتك في أي وقت قبل الاستبدال بعد نشر مفتاح الدخول الرئيسي KSK الجديد لمنطقة الجذر في 11 تموز (يوليو) 2017 والبعض قد يلقى بالفعل تحديثات آلية فعَّالة. والإجراء الذي تحتاج إلى اتخاذه يعتمد على ما يلي:

إذا كان برنامجك يدعم التحديثات الآلية لمرتكزات ثقة DNSSEC الامتدادات الأمنية لنظام اسم النطاق (RFC 5011):

يجب تحديث مفتاح الدخول الرئيسي KSK تلقائيًا في الوقت المناسب. لا يلزمك اتخاذ إجراء آخر.

تجدر الإشارة إلى أنه يجب تحديث الغير متصلة بالإنترنت أثناء الاستبدال يدويا إذا اتصلت بالإنترنت بعد انتهاء الاستبدال.

بدأت ICANN في تقديم منصة فحص ابتداء من مارس (آذار) 2017 للمشغلين أو لأي أصحاب شأن لتأكيد أن أنظمتهم تتعامل مع عملية التحديث الآلي بالطريقة الصحيحة. المزيد من المعلومات متوفرة على: **https://icann.org/kskroll.**

إذا لم يدعم برنامجك التحديثات الآلية لمرتكزات ثقة الامتدادات الأمنية لنظام اسم النطاق DNSSEC أو (RFC 5011) أو لم يتم تهيئته لاستخدامها:

يجب تحديث ملف مرتكز الثقة للبرنامج يدويا. يتوافر مفتاح KSK الجديد لمنطقة الجذر الآن هنا: **https://go.icann.org/2DOB7zn.**

متى يتم إجراء تغيير مفتاح توقيع شفرة الدخول الأساسية؟

استبدال مفتاح الدخول الرئيسي KSK عملية، وليس حدثا فرديا. التواريخ التالية مراحل رئيسية في العملية يتعرض المستخدمون النهائيون لانقطاع في خدمات الإنترنت:

11 تشرين الأول (أكتوبر) 2018

التاريخ المقترح لاستخدام مفتاح توقيع شفرة الدخول الأساسية الجديد للتوقيع للمرة الأولى.

11 يناير 2019

التاريخ المقترح لإلغاء مفتاح توقيع شفرة الدخول الأساسية القديم.

يمكن العثور على معلومات إضافية عن الاستبدال بما في ذلك الموارد لمساعدتك على الاستعداد للتغيير القادم على **https://icann.org/kskroll.**

يمكنك أيضا إرسال بريد إلكتروني إلى **globalsupport@icann.org** مع كتابة "KSK Rollover" في سطر الموضوع، أو الانضمام إلى المحادثة على Twitter باستخدام #KeyRoll.

2018 آذار (مارس) | Designed by ICANN Communications