DNSSEC (الامتدادات الأمنية لنظام اسم النطاق): تأمين نظام أسماء النطاقات DNS

مكتب المسؤول الفني الرئيس في ICANN

ديفيد كونراد
وثيقة OCTO-006v3
24 يوليو 2020

ICANN

قائمة المحتويات

هذه الوثيقة جزء من سلسلة مستندات مكتب المسئول الفني الأول. يُرجى الاطلاع على صفحة منشورات مكتب المدير الفني المسؤول OCTO للحصول على قائمة بالمستندات الموجودة في السلسلة. إذا كانت لديك أسئلة أو مقترحات حول أي من هذه المستندات، برجاء إرسالها إلى octo@icann.org.

تحتوي هذه المراجعة على مستجدات من العديد من الأشخاص الذين قرأوا وثيقة OCTO-006v2. تقدر ICANN بشكل كبير المراجعات المرسلة إلينا.

المقدمة

تساعد الامتدادات الأمنية لنظام اسم النطاق (DNSSEC) في تأمين طريقة انتقال المعلومات في جميع أنحاء الإنترنت.

ويُستخدم نظام أسماء النطاقات (*DNS*) من جانب جميع من يتصلون بالإنترنت وغالبية الأجهزة المتصلة بالإنترنت كل يوم. ومن خلال استخدام عملية تلقائية تُعرف باسم البحث أو الحل، تتمثل إحدى الوظائف العديدة لنظام اسم النطاق في تخطيط أسماء سهلة التذكر (على سبيل المثال، example.com) ويربطها بأرقام فريدة تُعرف باسم عناوين بروتوكولات الإنترنت (IP) (على سبيل المثال؛ 192.0.2.189 أو 2001: DB8:107A:61F7). ثم تستخدم الأجهزة عناوين IP هذه لتحديد بعضها البعض والتواصل مع بعضها البعض. وبهذه الطريقة، تتم مقارنة DNS في الغالب بدليل هاتف أو قائمة جهات اتصال، من خلال ترجمة الأسماء إلى أرقام.

ماهي امتدادات DNSSEC؟

عندما تم إنشاء نظام أسماء النطاقات DNS في أوائل الثمانينيات، لم يكن الأمان هو محور التصميم. نظرًا لقرار التصميم الذي كان منطقيًا في ذلك الوقت، كان من الممكن للمهاجمين - في حالات نادرة - تقديم إجاباتهم الخاصة لعمليات البحث عن اسم النطاق بدلاً من ما قصده مالك المجال (المسجل). على سبيل المثال، بدلاً من الانتقال إلى موقع الويب الذي طلبته في متصفحك، قد يقوم أحد المهاجمين بخرق رسائل DNS لإعادة توجيهك إلى موقع ويب يبدو مثل موقع الويب الذي تريد الانتقال إليه، ولكن يتحكم فيه المهاجم بدلاً من ذلك. وفي التسعينيات، توصل مجتمع DNS الفني إلى الحل النهائي لهذه المشكلة، والمعروفة باسم الامتدادات الأمنية لنظام أسماء النطاقات أو *DNSSEC*.

كيف تعمل امتدادات DNSSEC؟

المسجل هو الشخص أو المنظمة التي تتحكم في المعلومات المرتبطة باسم نطاق، أي تعيين الاسم إلى العنوان والبيانات الأخرى. تسمح امتدادات DNSSEC للمسجلين بإجراء توقيع رقمي للمعلومات التي وُضعت في DNS؛ ويتيح ذلك للعملاء (على سبيل المثال؛ متصفح الويب الخاص بك) التحقق من أن استجابات DNS التي يتلقونها ردًا على طلبات البحث لم يتم تعديلها منذ توقيعها.

في عام 2010، قامت ICANN بتمكين أعلى مستويات نظام اسم النطاق DNS، والمعروفة باسم الجذر، ليكون موقعًا من خلال DNSSEC، مما يسهّل إلى حد كبير نشر امتدادات DNSSEC عالميًا. وعلى الرغم من ذلك، وحتى بعد مرور قرن من الزمان، لا يزال نشر امتدادات DNSSEC متباطئًا.

ما هي فوائد نشر امتدادات DNSSEC؟

- **توفر الامتدادات الأمنية لنظام اسم النطاق الحماية للإنترنت**: ونظرًا لأن نظام أسماء النطاقات DNS ضروري لتشغيل الإنترنت، فإن حماية البيانات المقدمة من DNS أمر بالغ الأهمية. وقياسًا على ذلك، يمكن النظر إلى DNS باعتبارها إشارات مرورية على الإنترنت، بما يسمح بتوجيه الاتصال إلى المحتوى الصحيح أو الخدمة الصحيحة. وكما هو الحال مع إشارات المرور المتواجدة على الطرق الفعلية، إذا غيّر المهاجمون المكان الذي تشير إليه تلك العلامات، فقد يؤدي ذلك إلى ازدحام حركة المرور، وربما إعادة التوجيه إلى مكان سيء من المدينة.

- **توفر الامتدادات الأمنية لنظام اسم النطاق الحماية للمستخدمين**: يمكن لامتدادات DNSSEC أن توفر ضمانًا بأن بيانات اسم النطاق التي يتلقاها المستخدمون النهائيون هي نفس البيانات التي اعتزم المسجل أن يستلمها المستخدم النهائي. وتساعد امتدادات DNSSEC على ضمان أنه عندما يحاول مستخدم نهائي أو وسيلة الحصول على المحتوى أو الخدمة المشار إليها بواسطة اسم نطاق، فإن الموقع الذي يتصل به هو الموقع الذي قصده المسجل.

- **توفر الامتدادات الأمنية لنظام اسم النطاق الحماية للشركات والمنظمات والحكومات**: تقلل امتدادات DNSSEC من احتمال إساءة توجيه المستخدمين النهائيين الذين يرغبون في الاستفادة من خدماتهم أو مشاهدة محتواهم إلى موقع يمكن أن يتعرضوا فيه للاحتيال من قِبل المهاجمين. يمكن لمزودي خدمة الإنترنت (ISPs) إضافة قيمة إلى الخدمة التي يقدمونها لعملائهم من

خلال تمكين التحقق من DNSSEC على وحدات الحل لديهم. تقل مخاطر المنظمات التي توقع أسماء نطاقها باستخدام DNSSEC من حيث إساءة توجيه الأشخاص الذين يبحثون عنها على الإنترنت.

- **الامتدادات الأمنية لنظام اسم النطاق تدعم الابتكار**: توفر امتدادات DNSSEC طريقة للتحقق من بيانات DNS وحمايتها، مما يتيح الوثوق بتلك البيانات. وهذا بدوره يسمح للاستفادة من DNS العالمي في إنشاء قاعدة بيانات آمنة للأسماء/القيمة (على سبيل المثال؛ يمكنك تقديم اسم فيخرج لك DNS القيم المرتبطة بهذا الاسم ويمكن توزيع قاعدة البيانات هذه عالميًا ويمكن لأي شخص على الإنترنت الوصول إليها. ونتيجة لذلك، يمكن لقاعدة البيانات الآمنة هذه أن تستحدث فرصًا للابتكار وتمكّن التكنولوجيات والخدمات والوسائل الجديدة. على سبيل المثال؛ واحدة من هذه التقنيات، ألا وهي مصادقة الكيانات المسماة المستندة إلى DNS (DANE)، تستحدث طريقة جديدة لتأمين الاتصالات عبر الإنترنت. وتعمل تقنية DANE على الاستفادة من البيانات المحمية من DNSSEC في نظام أسماء النطاقات DNS وتعالج بعض نقاط الضعف بالطريقة الحالية التي يتم بها إجراء اتصالات آمنة على الإنترنت. وهذا ما يجعل التجارة عبر الإنترنت والاتصالات أكثر أمانًا.

كيف يمكنني تفعيل امتدادات DNSSEC؟

بشكل عام، لدى نظام أسماء النطاقات DNS جانبان: النشر، الذي يتم تنفيذه بواسطة المسجلين أو وكلائهم، والبحث (المعروف أيضًا باسم الحل)، والذي يتم عادةً بواسطة مشغلي الشبكات مثل مزودي خدمة الإنترنت. وللاستفادة من امتدادات DNSSEC، يجب على الجانبين استخدامه.

- **المسجّلون:** يجب على الأشخاص المسؤولين عن نشر معلومات DNS، التأكد من أن بيانات DNS الخاصة بهم موقعة من امتدادات DNSSEC. ومن الناحية التاريخية، تميل هذه العملية إلى أن تكون معقدة وعرضة للخطأ. ومع ذلك، تحتوي معظم حزم برامج وأنظمة تسجيل DNS الحديثة اليوم على أدوات تعمل على أتمتة توقيع DNSSEC على البيانات التي يرغب المسجّلون في نشرها. ونتيجة لذلك، يحتاج المسجلون أو وكلائهم فقط إلى تمكين تسجيل DNSSEC في خوادم DNS الخاصة بهم (أو لدى أمناء السجلات التي يتعاملون معها) وتقديم بعض المعلومات إلى أمين السجل الخاص بهم، والمعروفة باسم سجل موقّع التفويض، للمساعدة في وضع الثقة في المعلومات التي تم توقيعها للتو.

- **مشغلو الشبكات:** من ناحية البحث، بات الأمر أكثر سهولة: فلا يحتاج مشغلو الشبكات إلا إلى تمكين توثيق DNSSEC على وحدات حل البيانات التي تتناول عمليات بحث DNS لصالح المستخدمين. يمكّن برنامج وحدة الحل بشكل متزايد التحقق من DNSSEC بشكل افتراضي.

- **مستخدمو الإنترنت النهائيين:** لا يحتاج المستخدمون النهائيون عادةً إلى فعل أي شيء آخر غير تشجيع مشغلي شبكاتهم على تمكين التحقق من DNSSEC وتوقيع أسماء النطاقات التي يستخدمونها.

ما التكاليف المرتبطة بامتدادات DNSSEC؟

يتعين على خوادم DNS على جانبي النشر والبحث دعم DNSSEC، لذلك قد يكون من الضروري للمنظمات تحديث حزم برامج DNS الخاصة بها (وهي ممارسة مثلى، بصرف النظر عما إذا تم نشر DNSSEC أم لا).

- على ناحية النشر، قد يكون من الضروري أيضًا للمسجلين أو وكلائهم تعديل عملياتهم للسماح بإرسال سجلات "موقِّعي التفويض" إلى المسجل الخاص بهم. علمًا بأن تكلفة هذه التعديلات قد تكون كبيرة، ولكن هذا سيكون بمثابة تغيير وتكلفة لمرة واحدة.

- ومن ناحية البحث، على افتراض أن برنامج خادم DNS حديث إلى حد معقول، ينبغي أن تكون التكاليف ضئيلة حيث إن كل ما قد يلزم هو إجراء تغيير لمرة واحدة على التكوين لتمكين تحقق DNSSEC.

ماذا يحدث إذا لم أقم بنشر DNSSEC؟

- **قد يكون المستخدمون عرضة للهجمات:** إذا اختارت إحدى المنظمات عدم نشر أو تمكين DNSSEC، فإن مستخدميها عرضة لنوع معين من الهجمات يعرف باسم "التسمم المؤقت". فعندما يقوم المستخدم النهائي بالبحث، يمكن للمهاجمين إدراج إجابات على أسئلة DNS بشفافية، ومن المحتمل إعادة توجيه محاولات الاتصال إلى الأجهزة التي يتحكم فيها المهاجمون. يمكن للمهاجمين بعد ذلك تقليد مواقع الويب أو الخدمات الأخرى، وسرقة أسماء المستخدمين وكلمات المرور وما إلى ذلك، سيتم أيضًا الاحتفاظ بالإجابات غير الصحيحة في الخادم الذي يقوم بالبحث لفترة من الوقت، مما يؤدي إلى استمرار إعادة التوجيه حتى تنتهي صلاحية الإجابات أو تتم إزالته. في حين أن هذه الأنواع من الهجمات نادرة الحدوث، بالنظر إلى أن DNSSEC موجودة للتصدي لهذه الهجمات وكانت متاحة لبعض الوقت، فقد تضطر بعض المؤسسات التي وقعت ضحية لهذا الاستغلال إلى إجراء مناقشات حادة مع مستخدميها حول سبب عدم نشر DNSSEC. ونظرًا لمنع أشكال الهجوم الأخرى، فمن المحتمل أن يستفيد المهاجمون من المواقع التي لم تنشر DNSSEC حيث يصبح تنفيذ الهجمات عبر DNS أكثر شيوعًا.

- **قد يتعرض الابتكار للتباطؤ:** يؤدي عدم نشر امتدادات DNSSEC إلى إعاقة الابتكار وإبطاء نشر التقنيات الجديدة التي تستخدم DNS باعتباره قاعدة بيانات موثوق بها عالميًا. وتعِد بعض هذه التقنيات بتوفير طرق أفضل للثقة باتصالات خدمات الإنترنت، مثل البريد الإلكتروني أو الويب.

وعلى الرغم من وجود ثغرات أمنية في عنوان DNSSEC منذ إنشاء نظام أسماء النطاقات، فلا يزال هناك العديد من الهجمات البارزة التي تستفيد من هذه الثغرات الأمنية. ولهذا السبب، قد يعتقد البعض أن تكاليف نشر DNSSEC تفوق الفوائد التي توفرها امتدادات DNSSEC. ومع ذلك، تجدر الإشارة إلى أن تكاليف ومخاطر تنفيذ امتدادات DNSSEC قد انخفضت بشكل كبير. وفي الواقع، تتزايد فوائد امتدادات DNSSEC مع نشر المزيد من الشبكات لها.

طريقة أخرى للنظر في مسألة نشر امتدادات DNSSEC: "إذا كان الأمر يستحق الجهد المبذول لوضع البيانات في نظام أسماء النطاقات، ألا يستحق بذل الجهد لضمان عدم التلاعب بالبيانات؟"

بعض تاريخ DNSSEC

في عام 1983، نشر بول موكابيتريس من معهد علوم المعلومات في جامعة جنوب كاليفورنيا سلسلة من الوثائق التي قدمت مفهوم نظام اسم النطاق. لم يكن لدى DNS في شكله الأصلي في الثمانينيات، أي أمان أو سرية أو مصادقة مدمجة؛ لم تكن هناك آلية للتأكد من أن الإجابة التي تم تلقيها مشروعة وتتوافق فعليًا مع السؤال المطروح.

حوالي عام 1990، كتب ستيف بيلوفين من مختبرات بل التابعة لشركة AT&T ورقة تصف كيف يمكن للمهاجمين الاستفادة من قرار تصميم معين في DNS لاقتحام الأنظمة. أوصى بيلوفين في ورقته باستخدام مصادقة التشفير لحماية DNS بشكل أفضل. بعد نشر ورقة بيلوفين، بدأت عملية رسمية لجعل اقتراحه معيار بروتوكول فرقة عمل هندسة الإنترنت (IETF) المسمى "تحسينات أمان DNS" (*DNSSEC*).

تم تطوير برنامج DNS الذي قام بتنفيذ DNSSEC مبدئيًا في أواخر التسعينات، مع بعض عمليات النشر المبكرة لـ DNSSEC بدءًا من عام 2000 تقريبًا، بما في ذلك عن طريق .SE ccTLD الشهير (رمز بلد السويد). ومع ذلك، كشفت عمليات النشر المبكرة هذه عن العديد من التحديات التقنية لتشغيل DNSSEC على نطاق واسع في الإنتاج، مما أدى إلى استمرار IETF في العمل على تحسين البروتوكول على مدى السنوات الثماني القادمة.

لم يحدث شيء كبير من حيث النشر حتى عام 2008، عندما اكتشف باحث أمني يُدعى دان كامينسكي عيبًا خطيرًا في التصميم في بروتوكول DNS نفسه والذي سمح للمهاجمين بشن هجمات تسمم ذاكرة التخزين المؤقت ضد جانب البحث في DNS. حفزت هذه النتيجة محاولات متجددة من قبل مجتمع DNS الفني للحصول على المزيد من نشر DNSSEC، وعلى وجه الخصوص، في الحصول على جذر DNS الموقّع.

في تموز (يوليو) 2010، تم التوقيع على منطقة الجذر لأول مرة من قبل ICANN، مما يوفر مرتكز ثقة عالمي لجميع عمليات التحقق من DNSSEC. في تشرين الأول (أكتوبر) 2018، تم تحديث مفتاح التوقيع الرئيسي لمنطقة الجذر بنجاح للمرة الأولى، مما يمثل علامة بارزة مهمة لـ DNSSEC.

أدت سلسلة من حملات سرقة DNS الدولية في 2018 و2019 إلى أول توجيه للطوارئ على الإطلاق من قبل وكالة الأمن السيبراني الأمريكية وأمن البنية التحتية (US-CERT)، ودفعت ICANN إلى تجديد دعوتها لجميع أصحاب المصلحة في DNS لنشر DNSSEC بالكامل.

دور ICANN في DNSSEC

لطالما كانت ICANN، كجزء من مهمتها في الترويج لنظام DNS أكثر استقرارًا وأمانًا ومرونة، من المؤيدين الرائدين لنشر DNSSEC منذ فترة طويلة. تتطلب اتفاقيات التشغيل الرسمية الخاصة بـ ICANN مع كل من السجلات وأمناء السجل دعم DNSSEC. تتفاعل مؤسسة ICANN بانتظام مع أصحاب المصلحة في DNS حول العالم لمساعدتهم على فهم أهمية DNSSEC وتدريب المهندسين على كيفية نشر DNSSEC وتشغيلها في شبكاتهم. بالإضافة إلى الوعي وتنمية القدرات، يعمل التقنيون في ICANN مع مجتمع IETF على تحسينات DNSSEC.

من الناحية التشغيلية، تستمر ICANN في لعب دور حاسم. تعد ICANN مسؤولة عن إنشاء مفتاح توقيع مفتاح الجذر وتخزينه وتحديثه بشكل دوري، وهو مفتاح تشفير موثوق به من قِبل جميع المحللين المتحققين منه على الإنترنت، والذي يُستخدم في عملية التوقيع على جذر DNS العالمي.

لمزيد من المعلومات

هناك العديد من الموارد والمجموعات الفنية المشاركة في امتدادات DNSSEC ونشرها. عينة صغيرة:

- تتم مناقشة امتدادات DNSSEC وجميع الجهود الأخرى ذات الصلة ببروتوكول DNS ضمن فريق مهام هندسة الإنترنت (IETF)، وعلى وجه الخصوص في مجموعة العمل على عمليات DNS (مجموعة DNSOP).
- وتعقد ورش عمل امتدادات DNSSEC ثلاث مرات في السنة خلال اجتماعات ICANN العامة. وتوفر ورش العمل هذه - التي تنظمها جمعية الإنترنت - رؤى تشغيلية ومشورات وتحليلات حول نشر امتدادات DNSSEC. ثمة موقع مرتبط على الويب تحت رعاية جمعية الإنترنت يوفر أرشيفًا من تلك الاجتماعات.
- للحصول على مزيد من المعلومات، توفر ICANN وصفًا عامًا لامتدادات DNSSEC والسبب وراء أهميتها.