Neue DNSSEC-Schlüssel für die Root-Zone

Siegeltausch

Lutz Donnerhacke

Am 17. Oktober 2017 werden die Hauptschlüssel des Internets ausgetauscht. Im Idealfall werden die meisten Anwender davon nichts merken. Doch Systemverwalter sollten zumindest prüfen, ob sie Vorbereitungen treffen müssen – und worin diese bestehen.

Die Kurzfassung für Eilige lautet: Man startet den Test auf der Webseite https://dnssec.vs.uni-due.de/. Scheitert er, hat sich das Problem erledigt, denn DNSSEC ist dann für die eigene Domain (noch) kein Thema. Wer allerdings bereits eine für DNSSEC ausgelegte IT administriert, sollte nun handeln: Überall dort, wo die zentralen Schlüssel des weltweiten Domain Name System (DNS) hinterlegt sind, gilt es, einen Wechsel vorzubereiten.

Um zu verstehen, warum diese Schlüssel so besonders sind, muss man kurz ausholen. Als Beispiel diene der DNSSEC-Status von www.heise.de: www.heise.de selbst ist nicht mit DNSSEC gesichert (Abbildung 1). Aus der Delegation der de-Zone ergeben sich nicht nur die für heise.de zuständigen Nameserver, sondern auch, dass keine Schlüssel in dieser Zone bekannt sind (NSEC3). Damit kann der Resolver den Namen guten Gewissens ohne weitere Überprüfung nachschlagen (im DNS-Jargon „auflösen“).

Der Resolver hat von den DNS-Root-Servern erfahren, welche Nameserver für die de-Zone zuständig sind. Diese wiederum haben ihm mitgeteilt, dass es einen Schlüssel 39227 gibt (DS). Tatsächlich enthält die de-Zone diesen Schlüssel. Mit ihm hat sie den Arbeitsschlüssel 37704 signiert. Und dieser seinerseits hat den NSEC3 für heise.de unterschrieben. All das kann der Resolver überprüfen.

Der Resolver erhält seine Informationen über die Root-Zone schlicht aus seiner lokalen Konfiguration, in der unter anderem die Root-Nameserver eingetragen sind. Beim Starten liest der Resolver diese Daten von seiner Festplatte. Von dort bezieht er auch den Root-Schlüssel, den Hauptschlüssel des Internets. Der existiert seit 2010 unter der Kennung 19036. Mit ihm wurde der Arbeitsschlüssel 15768 unterschrieben, der seinerseits den DS-Eintrag (Delegation Signer) für die de-Zone signierte. Damit diese Validierung klappt, muss vom Beginn der Kette an immer der richtige Schlüssel gefunden werden. Und genau diesen zentralen Aufhängepunkt gilt es nun zu wechseln.

Für Systemverwalter kann das einiges an Arbeit nach sich ziehen: Überall dort, wo der Root-Schlüssel auf der Festplatte hinterlegt ist (als Hash, Hexstring, einkompiliertes Binärmaterial, Registry-Key etc.), muss zusätzlich der neue Schlüssel eingetragen werden – und zwar weltweit auf allen Geräten mit Internetanschluss: auf dem DSL-Router, dem Handy, dem vernetzten Kühlschrank, dem Auto(-Navi), der aus dem Internet steuerbaren Heimvernetzung, umfärbbaren Leuchtmitteln, Kraftwerken, Industrieanlagen und endlos so weiter.

Automatisierung als Standard

Damit diese Umstellung nicht zu einem Albtraum ausartet, gibt es seit 2007 den RFC 5011. Dieser besagt im Wesentlichen, dass der neue Schlüssel in der betreffenden Zone vorab veröffentlicht und unterschrieben werden soll. Ein spezielles Flag markiert ihn als Hauptschlüssel der DNS-Zone, als „Key Signing Key“ (KSK). Dem Arbeitsschlüssel fehlt das Flag, er heißt „Zone Signing Key“ (ZSK).

Sobald ein Resolver feststellt, dass es in einer Zone zwei Hauptschlüssel gibt und diese mit den aktuell gültigen Schlüsseln unterschrieben sind, lernt er den zusätzlichen Schlüssel und speichert ihn auf seine Festplatte. Wechselt dann irgendwann einmal die Zone den Schlüssel, kennt er den neuen, nun gültigen Schlüssel bereits.

Nachdem keine Signaturen mit dem alten Hauptschlüssel mehr existieren können, weil deren Gültigkeitszeiten überschritten sind, wird der alte KSK mit einem Löschbit markiert. Dieses signalisiert dem Resolver, dass er den alten Schlüssel von seiner Festplatte löschen kann.

Auf diese automatisierte Vorgehensweise setzt man beim Wechsel des Root-KSK, des Hauptschlüssels des Internets. Allerdings weiß man auch, dass viele Systeme entweder das Verfahren nicht beherrschen, gar nicht oder fehlerhaft konfiguriert sind. Ein exzellentes Beispiel dafür ist die anfangs erwähnte Webseite zum Selbsttest: Sie beschreibt in den Anleitungen für den DNS-Resolver Unbound eine RFC-5011-konforme Konfiguration. Die Anleitung für Bind dagegen enthält einen fest hinterlegten Schlüssel. Spätestens nach dem Wechsel des Hauptschlüssels im Oktober wird diese Seite also fehlerhafte Informationen liefern. Derzeit korrekt wäre eine Anleitung, die zumindest beide Schlüssel konfiguriert, optimalerweise bei Bind mit der Option „managed-keys“.

Erfahrungsgemäß kann es trotz vermeintlich korrekter Konfiguration vorkommen, dass der Schlüsselwechsel aus

einem trivialen Grund nicht klappt: wenn der Resolver nicht das notwendige Schreibrecht im Dateisystem hat. Er kann die Änderung nach RFC 5011 dann also gar nicht speichern.

Tücken des Testens

Bei oberflächlicher Betrachtung stellt sich die Frage, was denn daran so schlimm sein kann, im Rahmen der Umstellung hier und da ein System zu übersehen. Voraussichtlich wird sich dieses etwas merkwürdig verhalten, der Administrator merkt das irgendwann, erinnert sich an den Umstelltag und behebt den Fehler remote. Doch die Auswirkungen einer ungültigen Root-Zone können weitaus gravierender sein: Ich hatte testhalber schon vor dem offiziellen Signiervorgang eine signierte Root betrieben. Wegen eines Skriptfehlers wurden allerdings die Unterschriften der Nameserver-Einträge nicht erneuert. Am zweiten Weihnachtsfeiertag abends funktionierte dann gar nichts mehr. Keine E-Mail. Keine Webseiten. Auch kein Remotezugriff. Ich musste an den Konsolen sämtlicher betroffenen Rechner händisch die Validierung deaktivieren. Erst dann ließ sich der Fehler beheben.

Aus operativer Sicht ist ein Wechsel alle paar Jahre sinnvoll (siehe Kasten „Gründe für den Schlüsselaustausch“). Den Arbeitsschlüssel kann und sollte man sogar alle paar Monate tauschen. Dieser erzeugt den Hauptteil an Signaturen, ist also deutlich häufiger in Benutzung. Koordinieren muss man dazu fast nichts, denn der ZSK wird mit dem Hauptschlüssel der eigenen Zone unterschrieben. Der Wechsel erfolgt sozusagen in Personalunion. Nur darf man die externen Caches nicht vergessen, die DNS-Daten stunden- bis tagelang aufbewahren können.

Beim Tausch des KSK wird es komplizierter, denn auf diesen Schlüssel verweist ja die delegierende Elternzone. Hier muss man in koordinierter Weise über den eigenen Registrar die DS-Einträge in der Registry (für heise.de die für die de-Zone zuständige DENIC) so anpassen, dass jederzeit eine Validierung weltweit möglich ist.

Die meisten Registries verfahren nicht gemäß RFC 5011, lernen also nicht automatisch, dass es neues Schlüsselmaterial gibt. Stattdessen verlangen sie eine explizite Pflege der Einträge über die entsprechenden Programmierschnittstellen – man wende sich dafür also an seinen Reseller.

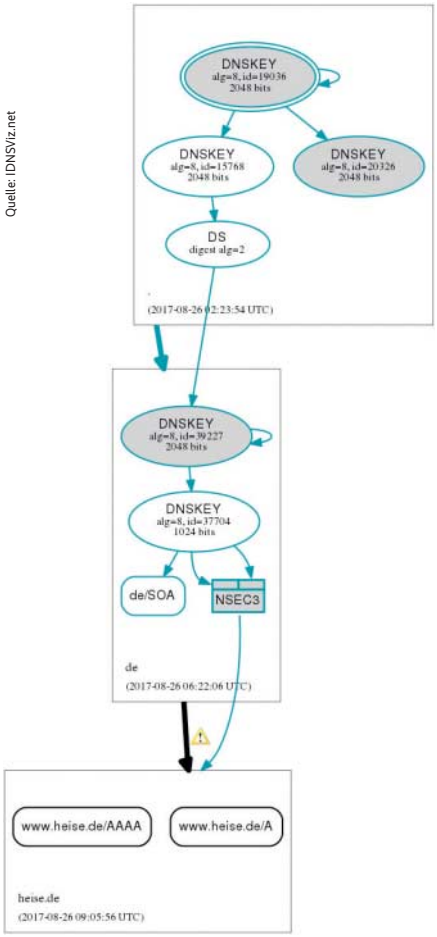
Wer den Ärger mit der externen Umstellung minimieren will, veröffentlicht daher zuerst den neuen Hauptschlüssel und nimmt damit beide KSKs parallel in Betrieb. Erst wenn diese neue Zoneninformation weltweit verfügbar ist, trägt man beim Registrar den DS-Eintrag auf den neuen Hauptschlüssel um und löscht nach einer angemessenen Schamfrist von einigen Tagen bis Wochen den alten KSK.

Eine andere Variante besteht darin, schon frühzeitig den neuen DS-Eintrag zusätzlich in der Registry zu veröffentlichen, um im Falle einer Kompromittierung den vorbereiteten Ersatzschlüssel sofort austauschen zu können. Details zu derlei Überlegungen finden sich in RFC 6781.

Diese Sichtweise lässt sich jedoch nicht auf den Hauptschlüssel der Root-Zone übertragen. Es gibt keine Registry, an die man sich wenden könnte. Die eine Registry, in der der Root-KSK steht, besteht praktisch aus Abermillionen von Geräten, die einen DNSSEC-validierenden Resolver betreiben. Hier sind die Umsetzung von RFC 5011 und viel Aufklärungsarbeit nötig. Jeder Anwender ist Teil dieser Registry und muss zum Ändern der Konfiguration bewegt werden.

Aber es gibt noch eine andere zu ändernde Registry. Der Hauptschlüssel des Internets, der Root-KSK, ist von so immenser technischer und politischer Bedeutung, dass die ICANN als koordinierende Institution beschlossen hat, die Schlüsselhoheit aufzuteilen: Die Hauptschlüssel werden über sieben Smartcards verteilt, die in jeweils eigenen Tresoren eingeschlossen sind. Zugang zu den Tresoren gibt es nur, wenn ein ICANN-Mitarbeiter ein Schloss und ein aus der weltweiten Kryptogemeinde stammender „Crypto Officer“ ein weiteres Schloss öffnet. Mit drei der sieben Smartcards kann ein Hardware-Security-Modul (HSM) den benötigten Schlüssel zusammensetzen und die vorgesehenen Unterschriften generieren. Die HSMs sind jeweils in eigenen Tresoren eingeschlossen.

Quelle: DNSViz.net



DNSViz unterstützt die Ursachenforschung, wenn Komplikationen bei der DNSSEC-Konfiguration eintreten (Abb. 1).

Aufgrund der ungewöhnlichen Komplexität des Vorgangs spielt sich das Ganze als live im Internet übertragene Zeremonie ab. Die Technik steht in eigens dafür vorgesehenen Sicherheitsräumen und es gibt vollständige Protokolle aller Vorgänge. Der zuvor festgelegte Ablauf der Zeremonie ist minutengenau zu protokollieren und jeder Einzelschritt zu unterschreiben. Auch diese Protokolle sind alle veröffentlicht.

Selbstverständlich muss es für den Katastrophenfall ein Ersatzsystem geben. Also existieren zwei dieser Einrichtungen: eins an der Ost- und eins an der Westküste der USA. Für beide sind unterschiedliche Crypto Officers zuständig. Da es einen

Quelle: IANA

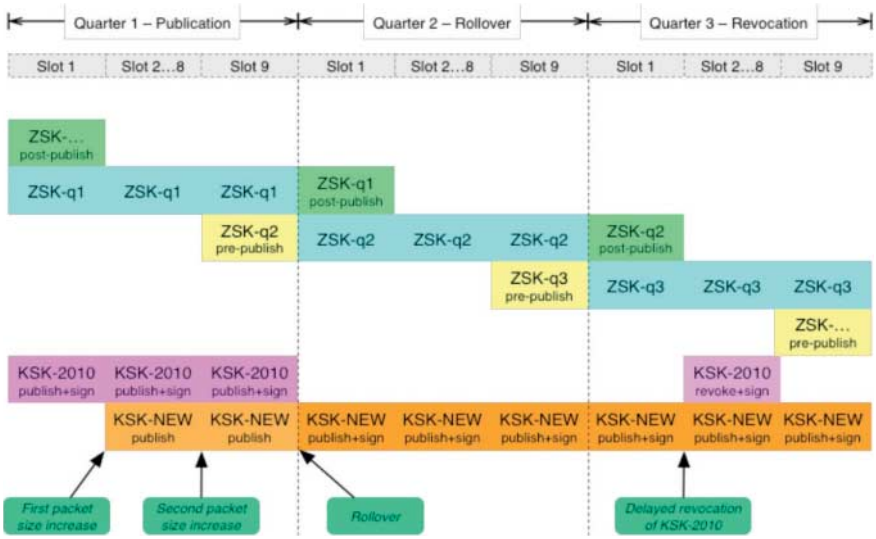
Im Oktober 2016 wurde der Schlüssel erzeugt, der nun aktiviert werden soll (Abb. 2).

Gründe für den Schlüsselaustausch

Angesichts der nebenstehend beschriebenen Risiken stellt sich eine sehr berechtigte Frage: Warum sollte man die zentralen Schlüssel für DNSSEC überhaupt wechseln? Die Schlüssel für eine gewöhnliche DNS-Zone werden beim Einrichten von DNSSEC tatsächlich normalerweise nur einmal erzeugt und existieren dann so lange, bis die Zone gelöscht wird.

Asymmetrische kryptografische Schlüssel sind jedoch prinzipiell knackbar. Und je häufiger Schlüssel zum Einsatz kommen, desto höher das Risiko, dass sie jemand knackt. Wie bei allen Kryptosystemen gibt es also eine gewisse maximale Anwendbarkeit eines Schlüssels. Umgekehrt sind selbst triviale Kryptosysteme sicher, wenn ihre Schlüssel nur ein einziges Mal verwendet werden (One-Time Pad). Dann muss der Schlüssel mindestens so lang sein wie die geheimen Daten.

Es ist also gute Praxis, die Schlüssel regelmäßig zu wechseln. Der Zeitraum dafür liegt je nach den im Einsatz befindlichen Schlüssellängen bei Monaten bis Jahren. Den Schlüsselwechsel gilt es ohnehin regelmäßig zu üben, um im Fall einer Kompromittierung (Fehlbenutzung, Publizieren bei GitHub, Diebstahl) des geheimen Schlüssels schnell und richtig reagieren zu können.



Quelle: IANA

Der aufwendige Prozess des Schlüsselaustauschs in der Root-Zone des DNS (Abb. 3)

hohen Aufwand bedeutet, diese aus aller Welt zusammenzutrommeln, findet die vierteljährliche Zeremonie abwechselnd in Ost und West statt. Die aus der Community stammenden Personen müssen also höchstens zweimal jährlich anreisen.

Für den Fall, dass die USA selbst nicht mehr sicher sind oder beide Einrichtungen zerstört wurden, gibt es eine Gruppe von sieben wiederum aus der Community ausgewählten Personen, deren Smartcards allerdings keine Tresore öffnen. Wenn fünf davon zusammenkommen, können sie eine neue Einrichtung mit neuen HSMs in Betrieb nehmen. Diese „Recovery Key Share Holder" reisen nicht regelmäßig, sondern nur auf Aufforderung – dann aber binnen Tagesfrist – an den Ort, der ihnen mitgeteilt wird.

Strikte Zeiteinteilung

Bei den vierteljährlichen Zeremonien wird ein Satz Unterschriften für den aktuellen Arbeitsschlüssel (ZSK) generiert, die jeweils immer nur drei Wochen gültig sind. Für den Zeitraum von drei Monaten werden dann Unterschriften des ZSK im Abstand von jeweils zehn Tagen erzeugt. Mit diesen Unterschriften kann der diensthabende Operator der Root-Zone alle zehn Tage der Arbeit nachgehen, zu der er nur den ZSK benutzt. Die passende Unterschrift des Hauptschlüssels hat er dann auf Vorrat. Auf diese Weise ist der Betrieb der Root-Zone quasi ein kurzfristig änderbarer Vertrag mit automatischer Kündigung.

Um in diesem Umfeld einen Hauptschlüssel überhaupt wechseln zu können, muss jede der Smartcards von ihrem zugehörigen Crypto Officer in einer Zeremonie aktualisiert werden. Aus Gründen der Nachvollziehbarkeit erstreckt sich der Vorgang über mehrere Zeremonien, dauert also Monate.

Der neue Key Signing Key wurde im Rahmen der 27. Zeremonie am 27. Oktober 2016 erzeugt und in der 28. Zeremonie am 2. Februar 2017 erstmals in der Root-Zone veröffentlicht. Ab der 31. Zeremonie am 18. Oktober 2017 soll er schließlich aktiv sein. Zur 32. Zeremonie wird dann der alte KSK zurückgezogen und damit der Prozess gemäß RFC 5011 abgeschlossen.

Definition des Scheiterns

Angesichts eines solch komplexen Prozederes stellt sich die Frage, wie denn ein Scheitern festgestellt werden soll. Neben den offenkundigen Fehlern, die sich mithilfe entsprechender Testumgebungen vorab ausschließen lassen, kann es beim Einsatz in der breiten Masse zu unvorhersehbaren Störungen kommen.

Da während der Schlüsselwechsel beide Keys aktiv sind, werden die DNS-Datenpakete zum Beispiel sehr groß. Daher gibt es Berechnungen, welche Paketgrößen auf welchem Transportweg (IPv4, IPv6) auftreten werden und welche Software damit möglicherweise Schwierigkeiten hat.

Als Grenzwert für eine so gravierende Störung, dass ein Rollback notwendig wird, wurden 0,5 % der Internetnutzer 72 Stunden nach dem Wechsel festgelegt. Wenn also mehr als 16 Mio. Nutzer aufgrund der Umstellung nach drei Tagen immer noch offline sind, erfolgt eine Wiederherstellung des alten Zustands – aber dessen Signaturen sind ja eigentlich schon abgelaufen.

Also wird während des Rollover in den Zeremonien nicht nur der bereits erwähnte Satz an ZSK-Unterschriften erzeugt, sondern auch jeweils ein Satz mit dem Schlüsselmaterial vor der Änderung. Bis zum Abschluss des Rollover kann die Root-Zone also in dem Zustand weiterbetrieben werden, den sie vor der jeweiligen Zeremonie hatte.

Der Erfolg des Unterfangens hängt entscheidend von den IT-Verantwortlichen in den Unternehmen, Universitäten und Haushalten ab: Sie müssen schlicht und ergreifend die Hauptschlüssel des Internets rechtzeitig aktualisieren, falls sie DNSSEC nutzen. Ich zähle auf Sie. (un)

Lutz Donnerhacke

hat bei der IKS Service GmbH Jena frühzeitig DNSSEC für den produktiven Kundenbetrieb eingeführt und bietet Consulting und Schulungen rund um DNSSEC an.

Alle Links: www.ix.de/ix1710116