Newsletter Oktober 2018

- DNSSEC Schlüsseltausch
- Englands Cyberangriff auf Belgien
- Wurde meine E-Mail kompromittiert?
- Neues von den Domains: .dk und Donuts

DNSSEC Schlüsseltausch

Der Nameservice ist eine Basistechnologie, ohne die das Internet zusammenbrechen würde. Anfangs war nur wichtig, dass es zuverlässig funktioniert; seit den 2000er Jahren spielen auch Sicherheitsaspekte eine Rolle.
Darum wurde DNSSEC erfunden, das den Nameservice absichert. Das geschieht mithilfe kryptographischer Signaturen, die als 'Chain of Trust' angelegt sind – jede Ebene vertraut der digitalen Unterschrift der nächsthöheren, ähnlich wie bei einem SSL-Zertifikat. Auf allen Ebenen werden die digitalen Unterschriften bzw. die zugrunde liegenden Schlüssel regelmäßig getauscht um Fälschungen vorzubeugen.
Ausgerechnet für die oberste Ebene, auf der das gesamte System aufbaut, gab es noch nie einen Schlüsseltausch. Das hängt damit zusammen, dass ein Tausch relativ einfach ist, wenn man der nächsthöheren Ebene mitteilen kann, dass sich etwas geändert hat. Für die oberste Ebene geht das natürlich nicht. Zwar hat man sich vor einiger Zeit auf ein passendes Verfahren geeignet. Problematisch ist aber, dass jeder einen Nameserver betreiben darf, ohne dass es eine zentrale Einrichtung gibt, die eine Liste von Nameserverbetreibern vorhält. Dadurch lässt sich nicht feststellen, ob alle das Verfahren beachten und nach einem Schlüsseltausch auf oberster Ebene weiter funktionieren.
Deswegen hat sich der Schlüsseltausch mehrfach verzögert. Jetzt will die zuständige IANA Ernst machen und den Tausch am 11. Oktober um 17 Uhr MEZ durchführen.
Wenn Sie selbst einen Nameserver betreiben, stellen Sie sicher, dass Sie auf den Schlüsseltausch vorbereitet sind. Kritisch sind dabei insbesondere zentrale Web-Virenscanner, die mit eigenem Nameservice ausgestattet sind. Sollten Sie ab dem Abend des 11. Oktober feststellen, dass wichtige Webseiten nicht mehr erreichbar sind, liegt wahrscheinlich ein Nameserverproblem vor.
Wenn Sie Ihren Internetzugang bei Global Village haben und entsprechend unsere Nameserver nutzen, sind Sie vor solchen Problemen gefeit.

Englands Cyberangriff auf Belgien

Im Rahmen der Snowden-Enthüllungen kamen auch Informationen ans Licht, die einen Spähangriff der GCHQ, des britischen Pendants zur NSA, auf den belgischen Provider Belgacom nahe legen. Ziel waren dabei die Belgacom-Kunden Europäische Kommission, Europäisches Parlament und Europäischer Rat. Es fanden gezielte Angriffe auf zentrale Belgacom-Mitarbeiter statt, die zur Infektion von 70 Arbeitsplätzen des Providers sowie zentraler Cisco-Router führte.
Dazu stellte die belgische Staatsanwaltschaft nun ihren Abschlussbericht vor. Dieser deutet darauf hin, dass die Angriffe von höchster Stelle in der Regierung genehmigt wurden. Damit handelt es sich um den ersten bekannten Angriff eines EU-Mitgliedes auf ein anderes.
Welche Daten dabei erspäht wurden, ist nicht öffentlich bekannt.

Wurde meine E-Mail kompromittiert?

Die Mozilla Foundation, unter anderem Herausgeber von Firefox und Thunderbird, gibt E-Mail-Nutzern eine einfache Überprüfungsmöglichkeit, ob ihre Adresse auffällig wurde. Interessierte können auf https://monitor.firefox.com eine Prüfung veranlassen. Besonders interessant ist die Möglichkeit, sich auch zukünftig informieren zu lassen, wenn die eigene Adresse als gehackt gilt.
Im Hintergrund bedient sich Mozilla bei der Datenbank HaveIBeenPawnd, die mittlerweile über 5 Milliarden (!) Einträge umfasst. Die Nutzung ist kostenlos.

Neues von den Domains

.dk

Die dänische Registry hat den Registrierungsprozess so vereinfacht, dass Domains direkt wie bei anderen Registries üblich, online beantragt werden können. Spätere Änderungen müssen aber weiter wie bisher im „Self Service"-Portal von DK Hostmaster vorgenommen werden, eine Verwaltung durch den Registrar ist immer noch nicht möglich.

Donuts

Der weltgrößte Anbieter von nTLDs mit einem Portfolio von 238 Domainendungen hat sich erst 2017 durch den Zukauf von Rightside vergrößert, nur um jetzt vom Investor Abry Partners aus Boston aufgekauft zu werden. Als treibende Kraft hinter dem Aufkauf gilt Fadi Chehadé, der von 2012 bis 2016 Geschäftsführer bei ICANN war. Über den Kaufpreis wurde Stillschweigen vereinbart.
Für Besitzer von Donuts Domains ändert sich durch den Kauf nichts.

Mit freundlichen Grüßen
Ihr Global Village Team