Newsletter März 2017

- Der böse Zwilling ✔
- Künstliche Intelligenz gegen Pöbeleien ✔
- Neues von den Domains: Verisign und .de ✔

Der böse Zwilling

Digitale Fingerabdrücke sind für die Sicherheit im Internet unerlässlich. Das Funktionsprinzip: Für beliebig große Dateien wird mittels eines mathematischen Verfahrens eine 'Prüfsumme' – der Fingerabdruck – mit einer festen Länge erstellt. Verändert man auch nur ein Bit in den Ursprungsdaten, so entsteht ein völlig anderer Abdruck.
Da der Fingerabdruck klein ist, kann es natürlich mehrere Dateien geben, die den gleichen Abdruck haben. Die Sicherheit des Fingerabdrucks entsteht dadurch, dass es sehr schwierig sein muss, zwei Dateien mit gleichem Abdruck zu erzeugen. Selbst wenn das gelingt, dürfen die Dateien keinerlei Ähnlichkeit aufweisen.
Das ältere SHA-1-Verfahren wird seit längerem von Krypto-Experten als nicht mehr ausreichend sicher angesehen, aber bisher waren die Missbrauchsmöglichkeiten eher theoretisch. Jetzt ist es Forschern gelungen, zwei ähnlich aussehende PDF-Dokumente mit gleichem Abdruck zu erzeugen. Damit entstand ein 'böser Zwilling': ein gefälschtes Dokument, das die digitale Unterschrift des echten trägt.
Der Aufwand war beträchtlich. Ein einzelner Computer hätte 6.500 Jahre für der Fälschung gebraucht. Dennoch dürfte das SHA-1-Verfahren Vergangenheit sein.
Im praktischen Einsatz findet man SHA-1 zum Beispiel bei SSL-Zertifikaten und der Nameservice-Absicherung DNSSEC. Wer noch auf das veraltete SHA 1 setzt, sollte bald auf den sicheren Nachfolger SHA-2 mit seinen Algorithmen SHA256 oder SHA512 umsteigen.
Global Village-Kunden können beruhigt sein. Wir haben vor mehr als einem Jahr das letzte von uns vergebene SHA-1-SSL-Zertifikat ausgetauscht. Noch entspannter ist die Situation bei DNSSEC. Hier kam von Anfang an mindestens SHA-2 zum Einsatz.
Es steht aber zu befürchten, dass im Netz noch vergessene Altlasten existieren, etwa selbst-signierte Zertifikate mit langer Laufzeit. Es ist nicht das drängendste Problem im Internet, aber ein Baustein, um das sich der jeweils Zuständige in absehbarer Zeit kümmern sollte.

Künstliche Intelligenz gegen Pöbeleien

Überall, wo diskutiert wird, gibt es auch Internetnutzer, die aus Machtstreben, Propaganda oder einfach nur Spaß provozieren, und das nicht selten jenseits der Grenzen des Anstands. Das ist insbesondere ein Problem für die Anbieter seriöser Medienangebote wie Nachrichtenmagazinen. Die Moderation von Onlineforen bindet viele Ressourcen.
Das Google-Projekt 'Jigsaw' will gestressten Redakteuren unter die Arme greifen. Ein auf einem neuronalen Netz basierender Bewertungsalgorithmus kann Texte einen 'Giftwert' von 0 (harmlos) bis 100 (Hasstirade) zuordnen. Ab einem Wert von 90 werden die Beiträge einem Bearbeiter zur manuellen Prüfung vorgelegt.
Es ist begrüßenswert, dass Werkzeuge wie dieses entstehen, und dass der Mensch die Entscheidungshoheit behält. Problematisch ist, dass Google wieder einmal mehr Daten erhält.

Neues von den Domains

Verisign Thick Whois

Die Registry Verisign wird für ihre TLDs .com und .net bis 2019 den 'Thick Whois' schrittweise einführen. Verisign ist die einzige namhafte Registry mit 'Thin Whois'. Beim 'Thick Whois' werden die Kontaktdaten einer Domain wie Domainregistrant und Domain-Administrator direkt bei der Registry gespeichert, beim 'Thin Whois' erledigt das der Registrar, über den die Domain registriert wurde, zum Beispiel Global Village.
Aus Verwaltungssicht ist die Umstellung vorteilhaft, da eine zentrale Datenbank mit allen Domaindaten einfacher zu handhaben ist. Das erleichtert zum Beispiel Domain-Transfers weg von unzuverlässigen Registrierern hin zu besseren Anbietern. Leider haben es aber auch Spammer leichter, E-Mail-Adressen einzusammeln. Und: Verisign ist U.S.-amerikanischer Anbieter und unterliegt damit der Kontrolle durch die National Security Agency (NSA), die Datenveränderungen somit ebenfalls einfacher durchleuchten kann.

.de Zonenupdates

Die .de Registry Denic verbessert sich. Bisher wurde die .de-Zone alle zwei Stunden aktualisiert. Dank neuer Hardware in den Rechenzentren in Frankfurt und Amsterdam halbiert sich diese Zeit. Updates von .de-Domains verbreiten sich damit doppelt so schnell.
Im internationalen Vergleich gibt es aber noch Luft nach oben. Viele Registries benötigen nur einige Minuten. Hier ist Verisign lobend zu erwähnen, die es trotz 150 Millionen verwalteter Domains schaffen, Updates nahezu in Echtzeit online zu stellen, und das inklusive der aufwändigen DNSSEC-Verschlüsselung.

Mit freundlichem Gruß,
Ihr Global Village Team