Newsletter Mai 2017

- Darf man Hacker hacken?
- Symantec SSL-Zertifikate von Herabstufung bedroht
- Neues von den Domains: .africa und .ro

Darf man Hacker hacken?

In Sicherheitskreisen wird derzeit ein Thema heiß diskutiert, das mehr als technische Argumente erfordert: Ist es statthaft, in unsichere Internetgeräte unerlaubt einzudringen und diese anschließend abzusichern?
Anlass ist die unfreiwillige Veröffentlichung von NSA-Spionagewerkzeugen, die im Untergrund auf fruchtbaren Boden gefallen ist. Eine Person oder Gruppe unter dem Pseudonym 'Shadow Brokers' ist hier besonders aktiv. Deren aktuelles 'Top-Produkt' Doublepulsar befällt Windows und soll bereits eine sechsstellige Zahl Rechner unter seine Kontrolle gebracht haben.
Nun lässt sich Doublepulsar aber auch nutzen, um in Systeme einzudringen, eventuellen 'bösartigen' Befall zu entfernen und das System danach abzudichten. Die Befürworter solcher Methoden argumentieren, dass die Besitzer wohl kaum etwas gegen eine Verbesserung der eigenen Sicherheitslage hätten. Gegner wiederum sind sich da nicht so sicher und fragen außerdem, wer haftet, falls das Abdichten zu Störungen bei einem vorher funktionierenden System führt. In den meisten Rechtsräumen ist so ein Vorgehen sowieso verboten. Insbesondere in Deutschland ist schon der Besitz derartiger Werkzeuge strafbar.
Vielleicht wird ein gutmeinender Robin Hood von einem Land mit laxer Gesetzgebung aus gegen die Hacker zu Felde ziehen. Und vielleicht werden wir nie davon erfahren.

Symantec SSL-Zertifikate von Herabstufung bedroht

Seit Symantec die Zertifizierungsstellen von Verisign und Thawte übernommen hat, ist das U.S.-Unternehmen einer der großen Anbieter von SSL-Zertifikaten, mit denen unter anderem die Übertragung von Webseiten verschlüsselt wird. Doch hat man es trotz hoher Preise mit der Prüfung der Kunden nicht ganz so genau genommen. So soll in den vergangenen Jahren eine fünfstellige Zahl von Zertifikaten unberechtigt ausgestellt worden sein.
Die Sicherheitsabteilung von Google liegt seit langem mit Symantec im Clinch und hat deren Praxis immer wieder angemahnt, nicht erst, seit 2015 ein falsches, auf google.com ausgestelltes Zertifikat im Umlauf war. Google droht, den hauseigenen Chrome-Browser so zu verändern, dass Symantec-Zertifikate der höchsten Sicherheitsstufe 'erweiterte Validierung' nur noch als einfache Zertifikate eingestuft werden. Der sichtbare Unterschied ist, dass in der Adresszeile nur noch ein Schloss-Symbol statt des Firmennamens des Webseiteninhabers erscheint.
Die Drohung zeigt Wirkung. Zwar will Symantec nicht der von Google vorgeschlagenen Transparenzinitiative beitreten, aber einmalig alle bereits ausgestellten Zertifikate durch einen externen Dienstleister prüfen lassen und sich außerdem regelmäßigen Audits der kanadischen WebTrust-Initiative unterziehen. Die Ironie besteht darin, dass Symantec selbst Adressvalidierung für Dritte anbietet, nun aber offensichtlich das Vertrauen in die eigene Qualität nicht mehr gegeben ist.
Ob sich Google dadurch besänftigen lässt, ist offen. In diesem Fall scheint der Internetgigant seine Marktmacht zur Verbesserung der allgemeinen Infrastruktur zu nutzen.
Global Village setzt übrigens nirgends Zertifikate von Symantec ein.

Neues von den Domains

.africa

Nach einer Schlammschlacht um Zuständigkeiten, in der eine der Parteien sogar Gottes Segen für sich geltend machen wollte, sind die Fronten nun geklärt. Die Südafrikaner von ZACR, unter anderem Betreiber der .za-Länderdomain, sind Registry der Kontinental-TLD .africa. Damit haben nach .eu, .asia (deckt auch den pazifischen Raum ab) und .lat alle Kontinente ihre eigene Domainendung – bis auf Nordamerika, wo man mit .com hinreichend zufrieden ist.
Markenrechtsinhaber können .africa bereits jetzt erwerben. Die allgemeine Verfügbarkeit beginnt am 3. Juli 2017.

.ro

Das rumänische NIC vertrat bisher das ungewöhnliche Konzept, Domains lebenslang gegen eine Einmalzahlung zu reservieren. Jetzt rudert die Registry zurück und führt regelmäßige Gebühren ein, auch für bereits bestehende Domains.
Dabei gilt für alle Registrierungen vor dem 1. Juli 2012, dass noch in der zweiten Jahreshälfte 2017 eine Zahlung fällig wird. Sollte diese nicht erfolgen, wird die Domain gelöscht. Für alle anderen gilt eine fünfjährige Schonfrist ab Registrierungsdatum.
Dass hier bereits geleistete Versprechen gebrochen werden, scheint in Bukarest niemanden zu stören. Als kleines Trostpflaster steht zu erwarten, dass einige interessante .ro-Domains demnächst gelöscht und damit wieder frei werden.

Mit freundlichen Grüßen

Ihr Global Village Team