Let’s Encrypt!

SSL/TLS-Zertifikate gratis für alle

Bild: Albert Hulm

Verschlüsselung einschalten – das kann jeder Webseiten- und Serverbetreiber. Damit alle Browser dieser Verschlüsselung vertrauen und keine Fehlermeldung anzeigen, muss eine Certification Authority (CA) ein Zertifikat unterzeichnen. Das macht Let's Encrypt narrensicher, vollautomatisch und kostenlos für jedermann.

Von Uli Ries

Kostenlose SSL/TLS-Zertifikate für alles und jeden – das Konzept von Let's Encrypt ist voll aufgegangen: Inzwischen weisen sich über 63 Millionen Domains mit einem Zertifikat der Gratis-CA aus, um verschlüsselte Verbindungen via HTTPS anbieten zu können. Let's Encrypt stellt inzwischen mehr SSL/TLS-Zertifikate aus als kommerzielle Dickschiffe wie Comodo oder DigiCert. Und durch Wildcard-Zertifikate (*.example.com) wird das Gratis-Angebot jetzt noch interessanter. Ist das Ende der kostenpflichtigen Anbieter nahe?

Davon träumt jedes Start-up: Binnen 24 Monaten nach der Gründung einen Markt aufzurollen und mehr Produkte unters Volk zu bringen als die seit Jahren etablierten Konkurrenten. Genau das ist dem Ende 2015 an den Start gerollten Projekt Let's Encrypt gelungen. Laut einer aktuellen Auswertung von NetTrack hat sich die Gratis-CA zur mit weitem Abstand beliebtesten Bezugsquelle für SSL/TLS-Zertifikate gemausert. Der Analysedienst hat für seine Erhebung versucht, verschlüsselte Verbindungen zu Servern aufzubauen, welche über rund drei Millionen Domains erreichbar sind. Gelang der Verbindungsaufbau, dann war in rund 40 Prozent der Fälle ein Zertifikat von Let's Encrypt im Einsatz. Comodo folgt weit abgeschlagen mit rund 20 Prozent, alle anderen CAs dümpeln im einstelligen Prozentbereich.

Hinter Let's Encrypt (LE) steckt die Internet Security Research Group (ISRG), der unter anderem Akamai, Cisco, die Electronic Frontier Foundation (EFF) und Mozilla angehören. Das Erfolgsrezept ist schnell erklärt: kostenlos und einfach. Die Initiative hat sich das Ziel gesetzt, die Verbreitung verschlüsselter Verbindungen auf 100 Prozent zu steigern. Dieses Ziel ist zwar noch längst nicht erreicht, die Richtung stimmt jedoch: Waren zum Start der Gratis-CA Ende 2015 – und damit gut 20 Jahre nach dem Start von HTTPS – knapp 40 Prozent aller Seitenaufrufe verschlüsselt, sind es heute mehr als 67 Prozent; dies geht laut LE aus den von Mozilla Firefox gemeldeten Telemetriedaten hervor. Google meldet sogar 73 Prozent. Welchen Marktanteil die Initiative dabei hat, ist nach Einschätzung von LE irrelevant für den Erfolg des Projekts. Daher will die Gratis-CA die NetTrack-Statistik auch nicht bestätigen.

Fest steht laut Let's Encrypt aber, dass 95 Prozent aller von LE ausgestellten Zertifikate Domains zugewiesen sind, die zuvor kein öffentlich sichtbares – und somit sehr wahrscheinlich gar kein – SSL/TLS-Zertifikat hatten. Unter den LE-Nutzern befinden sich inzwischen auch so illustre Organisationen wie die US-Raumfahrtbehörde NASA, die alleine knapp 1800 Zertifikate bei Let's Encrypt beantragt hat. Auch einige Gerätehersteller wie AVM und Synology haben LE für sich entdeckt und statten ihre NAS und Router mit einem LE-Client aus (siehe S. 84 und 85). Die kostenlosen Zertifikate kann man überall dort nutzen, wo TLS zum Einsatz kommt – also etwa auch auf dem Mailserver.

Licht – aber auch ein bisschen Schatten

Einer Sprecherin zufolge schreibt sich Let's Encrypt die zunehmende Verbreitung von TLS nicht alleine auf die Fahnen. Ähnlich sieht das auch Jeremy Rowley, leitender Produktmanager des Unternehmens DigiCert, welches das Zertifikatsgeschäft von Symantec übernommen hat. Seiner Meinung nach hat unter anderem Google entscheidend zum Zuwachs von HTTPS-Webseiten beigetragen: „Erst schob Google mit HTTPS gesicherte Webseiten weiter nach vorn in den Suchergebnissen. Ab Oktober 2017 begann Google dann, einige nicht verschlüsselt ausgelieferte Webseiten abzustrafen und als unsicher zu markieren", so Rowley gegenüber c't.

DigiCert hat mit Encryption Everywhere ein eigenes Gratis-Programm am Start, das aber nur durch Partner wie Hosting-Anbieter zugänglich ist. Genau wie bei Let's Encrypt sehe man, dass „die gratis ausgestellten Zertifikate von Betreibern kleinerer Domains genutzt werden, die andernfalls wahrscheinlich auf Verschlüsselung verzichten würden", so Rowley. Letztlich freue man sich bei DigiCert über den positiven Einfluss, den Let's Encrypt auf die Sicherheit im Web habe.

Rowley sieht aber auch Schwierigkeiten durch die unbegrenzte Verfügbarkeit von kostenlosen Zertifikaten: „Dies begünstigt Phishing und andere Online-Betrügereien. Denn die kostenlosen Zertifikate sorgen zwar für Verschlüsselung, liefern aber keine Angaben über die Identität des Domaininhabers oder Seitenbetreibers", sagt der DigiCert-Vertreter. Phisher liefern ihre gefälschten Login-Seiten vermehrt über HTTPS aus, um sich mit dem Schloss-Symbol in der Adressleiste des Browsers das Vertrauen ihrer Opfer zu erschleichen. Dass Kriminelle Let's Encrypt nutzen, legt ein im März 2017 veröffentlichter Report (siehe ct.de/y68u) nahe: Den Autoren zufolge stellte LE über 15.000 Zertifikate aus, in deren Domainnamen „paypal" auftauchte.

Bedrohung für kommerzielle Anbieter?

Böse Zungen behaupten, dass der besagte Report von Verkäufern kommerzieller Zertifikate verbreitet wurde. Denn zum einen wurden auch Gratis-Zertifikate von Comodo für Tausende von Phishing-Seiten ausgestellt. Zum anderen zeigen Reaktionen der Anbieter, dass die ihre Felle davon schwimmen sehen: Comodo versuchte im Herbst 2015 – und damit ein gutes Jahr, nachdem Let's Encrypt erstmals von sich reden machte –, Markenzeichen für „Let's Encrypt" oder „Comodo Let's Encrypt" registrieren zu lassen. Das Unternehmen zog die Anträge zwar zurück, ein bitterer Nachgeschmack bleibt jedoch.

Von W3Techs ermittelte Marktzahlen zeigen, dass die etablierten Anbieter wie Comodo, DigiCert (Symantec), GoDaddy oder GlobalSign in einem an sich wachsenden Markt bestenfalls stagnieren, in den meisten Quartalen seit dem Start von LE

jedoch Federn lassen mussten. Die inzwischen auf Rang zwei geführte IdenTrust-CA hingegen ist von nahe null auf 33 Prozent Marktanteil gewachsen. Der Erfolg geht ausschließlich auf Let's Encrypt zurück, da IdenTrust das Zwischenzertifikat (Intermediate) von Let's Encrypt per Cross-Signing gegengezeichnet hat. Als LE an den Start ging, vertrauten die Browser dem Wurzelzertifikat der jungen CA (ISRG Root X1) noch nicht – dem Root Certificate von IdenTrust hingegen schon. Nur das Cross-Signing verhinderte TLS-Fehlermeldungen.

1&1, Strato & Co.: DigiCert statt Let's Encrypt

Im deutschsprachigen Raum setzen bislang nur kleinere Hosting-Anbieter wie hostNet aus Bremen, Futureweb aus St. Johann (Österreich) oder die Wordpress-Hoster Hostpress und WLWP auf Let's Encrypt. Wer seine Webseiten bei einem der hiesigen Platzhirsche wie 1&1, Hetzner oder Strato hostet, kommt entweder gar nicht oder nur durch Eigeninitiative in den Genuss der kostenfreien LE-Zertifikate. So sagt ein Sprecher von Strato auf Nachfrage, dass man „Let's Encrypt bei den Webhosting-Paketen aktuell nicht unterstützt." Bei Server-Produkten von Strato sind zur Installation der LE-Zertifikate root-Rechte nötig (siehe ct.de/y68u). Ansonsten setzt Strato auf DigiCert, weil man „keine Kompromisse bei den Qualitätsansprüchen" eingehen wolle, so der Sprecher.

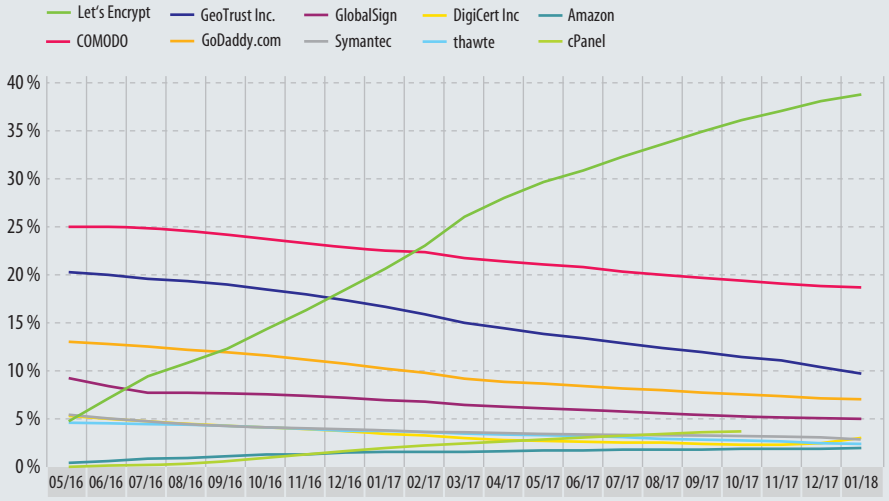
Seit Mai 2016 – also kurz nach dem Start von LE – biete Strato Nutzern des Hosting-Pakets, des Homepage-Baukastens, des Webshops und der Server stattdessen ein TLS-Zertifikat von DigiCert ohne Zusatzkosten an. Bei Managed Servern sei ein solches Zertifikat schon immer inklusive gewesen. Ähnliches lässt auch Hetzner verlauten: Webhosting- und Managed-Server-Kunden können kostenfreie DigiCert-Zertifikate bekommen. Let's Encrypt spielt für den Hoster keine Rolle.

Ebenso wenig bei Host Europe: Nutzern von Shared-Hosting-Produkten bietet das Unternehmen keine automatisierte Möglichkeit, ein externes Zertifikat zu verwenden. Man kenne Let's Encrypt zwar, richtet sich „jedoch vorrangig an Kunden mit hohen Sicherheitsanforderungen, die eine Komplettlösung inklusive umfassendem Versicherungsschutz" erwarten, so eine Sprecherin. Die hohen Sicherheitsanforderungen sollen Zertifikate der Stufen OV (Organization Validated) oder EV (Extended Validation) bieten, die Let's Encrypt nicht im Angebot hat.

Und auch 1&1 möchte „keine Kompromisse bei den Qualitätsansprüchen" eingehen, so ein Sprecher. Daher setze man auf eine enge Zusammenarbeit mit DigiCert.

Verbreitung von Let's Encrypt

Laut einer Auswertung von NetTrack hat sich Let's Encrypt zum mit Abstand meist genutzten Zertifikatsherausgeber gemausert.



Eine milde Gabe, bitte

Unter anderem über Twitter ruft Let's Encrypt regelmäßig dazu auf, der Initiative Geld zu spenden. Der Sprecherin zufolge gehören diese Spenden fest ins Finanzierungskonzept: Neben den Trägern wie Akamai, Cisco, Google, Mozilla und der Electronic Frontier Foundation spenden laut LE zirka 40 Sponsoren wie 3CX, Facebook oder ZenDesk sowie die Ford Foundation Geld.

Zusammen mit Spenden von Privatpersonen soll so genug Geld zusammenkommen, um die für das Jahr 2018 budgetierten Kosten in Höhe von 2,45 Millionen Euro zu decken. Obwohl dies laut LE lediglich einem Zuwachs um 13 Prozent gegenüber dem Vorjahr entspricht, sollen doppelt so viele Zertifikate ausgestellt werden wie im Jahr 2017. Die hierfür notwendige Hardware ist es, für die das zusätzliche Geld nötig wird.

ACME v2 und Wildcards

Wie Josh Aas, Executive Director der ISRG, schreibt, muss LE auf Automatisierung setzen, um das kleine Team zu entlasten und die Kosten unter Kontrolle zu halten. Daher hat LE mit dem Automated Certificate Management Environment, kurz ACME, ein Protokoll zum Automatisieren der Zertifikatsausstellung entwickelt. Es wird inzwischen von vielen Clients unterstützt, die nicht nur das signierte Zertifikat abrufen, sondern sich auf Wunsch auch um die Konfiguration des Servers kümmern. Die interessantesten Implementierungen für verschiedene Einsatzszenarien und den Einsatz in der Praxis stellen wir auf den folgenden Seiten vor.

Ende Februar soll ACME v2 an den Start gehen (siehe Seite 94), das sich derzeit noch im Probebetrieb befindet. Das Protokoll steht ausdrücklich auch anderen CAs offen und unterstützt nun auch endlich Wildcard-Zertifikate (also *.example.com), was Let's Encrypt weiteren Zulauf bescheren dürfte. Webmaster benötigen damit nur noch ein Zertifikat für eine Domain, um sämtliche Subdomains abzusichern. Kommerziellen Anbietern bleibt unterdessen nur noch das Geschäft mit Extended-Validation(EV)-Zertifikaten. Das Ausstellen dieser Zertifikate lässt sich nicht automatisieren, da Menschen die vom Antragsteller eingereichten Angaben wie Firmenname, Unternehmenssitz oder Domainbesitz von Hand kontrollieren müssen. Ob sich nur mit EV-Ausstellung ganze CAs gewinnbringend betreiben lassen, ist allerdings fraglich. *(rei@ct.de)* c't

Nettrack-Statistik: ***ct.de/y68u***