Let's Encrypt startet am 3. Dezember

Die Zertifizierungsstelle Let's Encrypt (siehe c't 25/15, S. 136) will am 3. Dezember in die öffentliche Beta-Phase übergehen. Ab dann will man kostenlose SSL-Zertifikate für jedermann ausstellen. Laut dem Leiter des Projektes hat die CA seit dem Start der geschlossene Betaphase bereits über 11 000 Zertifikate ausgestellt. Nach diesen Erfahrungen sind die Organisatoren zuversichtlich, dass die Systeme bereit für den öffentlichen Betrieb sind. Allerdings wollen die Entwickler noch an der Konfigurations-Software feilen – aus diesem Grund startet das Projekt auch für die Öffentlichkeit erst einmal im Beta-Modus.

Hinter Let's Encrypt stehen bekannte Firmen wie Mozilla, Akamai, Cisco und die Electronic Frontier Foundation. Sie haben sich zur Internet Security Research Group (ISRG) zusammengefunden und wollen verschlüsselte HTTPS-Verbindungen zum Standard im Web machen. Das Projekt will dies mit kostenlosen Zertifikaten erreichen, die von den gängigen Browsern als vertrauenswürdig eingestuft werden. (fab@ct.de)

Amazon führt Zwei-Faktor-Anmeldung ein

Der Online-Versandhandel Amazon bietet in den USA nun eine Anmeldung per Zwei-Faktor-Authentifizierung an. Nach der Aktivierung müssen Nutzer neben ihrer E-Mail-Adresse und ihrem Passwort zusätzlich einen Code eingeben, der per SMS aufs Handy gesendet oder über eine Authentifizierungs-App wie Google Authenticator oder Authy erzeugt wird. Das schützt davor, dass Angreifer das Konto kapern, falls die Anmeldedaten in falsche Hände gelangen.

In Deutschland ist das zusätzlich abgesicherte Anmeldeverfahren noch nicht verfügbar. Auf eine entsprechende Anfrage von c't hat Amazon bis zum Redaktionsschluss nicht geantwortet. Über einen Umweg kann man die Zwei-Faktor-Authentifizierung allerdings schon jetzt auch hierzulande nutzen. Dazu muss man sich mit seinen Anmeldedaten für die deutsche Amazon-Seite auf amazon.com anmelden und dort die Zwei-Faktor-Anmeldung aktivieren. Der zusätzliche Code wird ab dann auch bei Anmeldungen auf amazon.de abgefragt. (des@ct.de)

Sicherheits-Notizen

Eine drei Jahre alte Sicherheitslücke in den Versionen 5.1.4 bis 5.1.9 der Foren-Software **vBulletin** wird nun großflächig ausgenutzt. Administratoren sollten ihre Foren-Installationen unbedingt mit dem bei vBulletin verfügbaren Patch absichern.

Die VPN-Software **StrongSwan** weist eine Sicherheitslücke in ihrem EAP-MSCHAPv2-Plug-in auf. Ein Angreifer kann dadurch die Authentifizierung umgehen. In Version 5.3.4 wurde die Schwachstelle gestopft.

Die Bibliothek **libpng** zur Verarbeitung von PNG-Grafiken kann dazu missbraucht werden, Rechner lahmzulegen. Angreifbar sind die Versionen 1.0.63, 1.2.53, 1.4.16, 1.5.23 und 1.6.18 der Software. Updates beheben das Problem.