PSW GROUP

über 17 Jahre

CAA – Certification Authority Authorization

© Sergey Nivens / fotolia.com

Bei Certification Authority Authorization, kurz: CAA, handelt es sich um ein Verfahren, bei dem Sie als Domaininhaber im DNS festlegen, welche CA für Ihre Domain Zertifikate ausstellen darf und für das Validieren zuständig ist. Das im RFC 6844 dokumentierte Verfahren wird auch als CA-Pinning, Certificate Pinning oder SSL-Pinning bezeichnet. Dabei wird das SSL-/TLS-Zertifikat nicht nur an einen festgelegten Host sondern auch an eine festgelegte CA (Zertifizierungsstelle) gebunden.

Wozu ist CAA gut?

Das ursprüngliche Modell der Zertifizierungsstellen erlaubte es, dass jede CA für jeden Host- bzw. Domainnamen Zertifikate ausstellen kann. Das konnte zur Folge haben, dass mehrere Zertifikate von verschiedenen CAs für ein und dieselbe Domain ausgestellt werden.

Angreifer machen sich dies zunutze: Um einen Man-in-the-Middle-Angriff (MITM) zu starten, lassen sich Angreifer ein gültiges Zertifikat ausstellen, obwohl sie nicht Domain-Inhaber sind. Das erlaubt dem Angreifer, sich mit dem gefälschten Zertifikat als Server auszugeben, der er nicht ist. Man spricht hierbei vom Identitätsdiebstahl. So lassen sich auch verschlüsselte Verbindungen zwischen Server und Client übernehmen.

Ist nun ein Zertifikat eines Hosts bzw. einer Domain an eine vorher festgelegte Zertifizierungsstelle gebunden, fällt bereits beim Validieren auf, dass das Zertifikat von einer fremden CA gezeichnet ist. Dann wird das Zertifikat als ungültig angesehen.

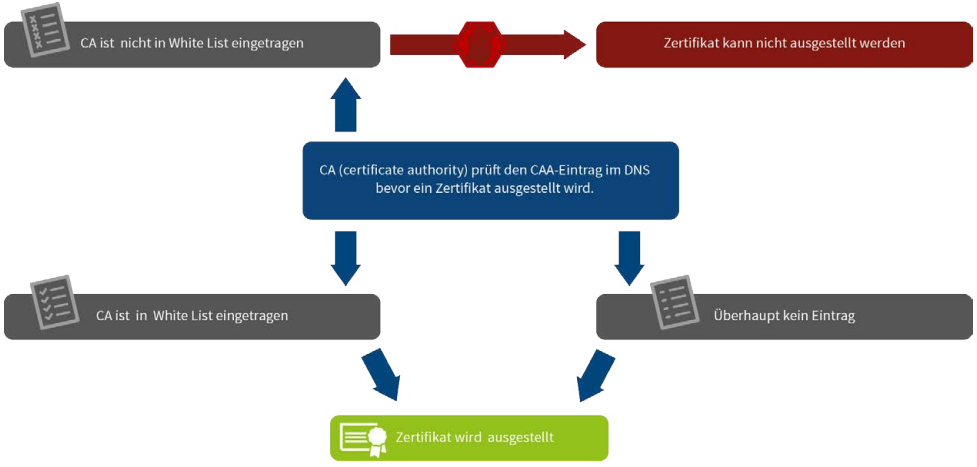
Und wie funktioniert CAA?

Schon in der DNS legen Sie als Domaininhaber mithilfe des CAA-Records fest, welche Zertifizierungsstelle ein Zertifikat für Ihre Domain ausstellen darf. Für diese Domain darf nun ausschließlich diese CA Zertifikate ausstellen. Es kann nicht mehr zu fälschlich ausgestellten Zertifikaten kommen.

Wurde das Zertifikat durch die richtige CA ausgestellt, kann diese Zertifizierungsstelle auch nach der Gültigkeit des TLS-Zertifikats befragt werden. Versucht nun eine Gegenstelle, sich als korrekter Server auszuweisen und präsentiert dafür ein Zertifikat, welches von einer anderen CA unterschrieben wurde, schlägt der Client Alarm.

Diese neue Regelung wurde in den Baseline Requirements festgelegt und ist wirksam ab dem 08. September 2017. Heißt: Ab diesem Stichtag können SSL/TLS-Zertifikate nur dann ausgestellt werden, wenn die CA als CAA in der DNS festgelegt wurde. Legen Sie kein CAA Record (= CAA-Eintrag) an, kann das Zertifikat von jeder CA ausgestellt werden. Ihrer eigenen Sicherheit zuliebe legen Sie in der DNS also ein CAA Record an.

Maßnahmen zum Schutz gegen unberechtigt zugestellten Zertifikaten



Certification Authority Authorization

Pro

- Verhindert Ausgabe von falschen Zertifikaten
- Erfordert keine Änderungen im Browser
- Keine hohen Implementierungskosten
- Meldemechanismen können Websitebesitzer warnen, wenn ein falsches Zertifikat ausgestellt wird

Kontra

- Koordinationsprobleme durch mehrere Administratoren

PSW GROUP: Mit Sicherheit Ihr Partner

Die PSW GROUP ist Ihr Full-Service-Provider für Internetlösungen mit einem besonderen Schwerpunkt auf Internet Security. Als Dienstleister bieten wir Ihnen sowohl für den Webeinsatz als auch für die E-Mail-Kommunikation maßgeschneiderte Zertifikats-, Signatur-, Verschlüsselungs- und Authentifizierungslösungen an. Unser voll umfassendes Produktportfolio reicht dabei von SSL-Zertifikaten über Code Signing-Zertifikate bis hin zu S/MIME-Zertifikaten.

Neben der großen Produktvielfalt verfügen wir über langjährige Expertise in den Bereichen Internetsicherheit und IT-Recht. Mit unserem tiefgreifenden und zertifizierten Fachwissen als IRCA ISO 27001 ISMS Lead-, Datenschutz- und IT-Security-Auditoren, Certified Information Systems Security Professionals , Security Manager, Cyber-Security Practitioners und Symantec Sales Experts Plus sowie Sophos Certified Architects, stehen wir Ihnen auch bei den komplexesten Fragestellungen beratend zur Seite.

+49 661 480276 10

info@psw-group.de

PSW GROUP
GmbH & Co. KG
Flemingstrasse 20-22
D-36041 Fulda

Phone +49 661 480276 10
Fax +49 661 480276 19
E-Mail info@psw-group.de
Internet www.psw-group.de