Zertifikate und CAA-Records

Der DFN-Verein stellt mit seinem Dienst DFN-PKI eine Public-Key-Infrastruktur bereit, um digitale Zertifikate auszustellen. Es handelt sich dabei um Zertifikate auf Basis des X.509-Standards, die Sie als DV-Koordinator aus dem KDD heraus über die Schnittstelle des Betreibers (aktuell Sectigo bzw. GÉANT Trusted Certificate Services) beantragen können. Mit den so ausgestellten Serverzertifikaten sichern Sie die Kommunikation der von Ihnen selbst betriebenen Serverdienste ab.

Wenn Sie solche Zertifikate aus der DFN-PKI im Einsatz haben, dann ist es für Sie von Interesse, dass der DFN mit einem neuen Mechanismus zur Validierung von Zertifikaten die Sicherheit der DFN-PKI weiter erhöht hat. Wer als DV-Koordinator in seiner Einrichtung Zertifikate der DFN-PKI einsetzt, muss dazu im Grunde nichts weiter beachten. Der DFN sorgt mit der DFN-PKI dafür, dass der Zertifikatseinsatz durch CAA Resource Records noch sicherer ist. Mit der Bereitstellung von CAA Resourde Records werden Anforderungen des CA/Browser-Forums umgesetzt, damit die Zertifikate aus der DFN-PKI weiterhin über das Wurzel-Zertifikat in den Internetbrowsern verankert ist.

Handlungsbedarf in Bezug auf CAA Resource Records im DNS an der TU Braunschweig besteht nur dann, wenn Zertifikate von anderen Zertifizierungsstellen eingesetzt werden sollen. Die Zulassung anderer Zertifizierungsstellen wurde sowohl intern als auch mit anderen Teilnehmern im DFN-Verbund diskutiert und sich dagegen entschieden. Die Beschränkung auf die DFN-PKI bringt es mit sich, dass ein Auftreten nach Außen im Namen der TU Braunschweig z.B. über Web-Dienste mit vertrauenswürdigen Zertifikaten nur mit entsprechender Genehmigung und Koordination möglich ist. Hier die Chance den Überblick - auch über ggf. begründet notwendige Ausnahmen - behalten zu können, ist u.a. eines der Anliegen, die sowohl von unserem CISO als auch an anderen Hochschulrechenzentren geteilt wird.

> Das Ausstellen/Signieren von Zertifikaten, die nicht aus der DFN-PKI (aktuell Sectigo/GÉANT TCS) kommen, ist für Hostnamen unterhalb von tu-braunschweig.de/tu-bs.de nicht möglich.

Der neue Mechanismus zur automatisierten Validierung von Zertifikatsanträgen durch die PKI-Betreiber setzt darauf auf, dass sogenannte CAA Resource Records im DNS einer Domain gesetzt sind. Dieser Mechanismus ist für jede im Browser verankerte Zertifizierungsstelle/PKI verpflichtend umzusetzen. Auf Anforderung des CA/Browser-Forums muss jede PKI vor der Ausstellung eines Zertifikats prüfen, ob im DNS einer Domain sogenannte CAA Resource Records nach RFC 6844 hinterlegt sind und diese auswerten.

Im Klartext bedeutet dies, dass im Rahmen der Ausstellung von Zertifikaten alle PKI-Betreiber über die CAA Resource Records automatisiert überprüfen müssen, ob sie für den Zertifikatsantragssteller bzw. dessen Domain autorisiert sind, Zertifikate zu signieren. Sind Zertifizierungsstellen/PKIs vom Domaininhaber nicht dazu autorisiert, dürfen sie entsprechende

Zertifikatsanträge nicht digital signieren.

Domaininhaber haben es damit in der Hand, durch Hinterlegen von CAA Resource Records zu verhindern, dass Zertifikate von nicht autorisierten Zertifizierungsstellen/PKIs ausgestellt werden. Bislang konnten weltweit alle im Browser verankerten Zertifizierungsstellen Zertifikate für jede beliebige Domain ausstellen. Dies hatte in der Vergangenheit immer wieder zu Missbräuchen geführt.

CAA Resource Records für die DFN-PKI wurden im DNS der TU Braunschweig hinterlegt. Insgesamt ist damit ein Missbrauch von Zertifikaten mit Domain-Namen der TU Braunschweig z.B. durch kompromittierte Zertifizierungsstellen unwahrscheinlicher. Auch wird es mittels der CAA Resource Records schwieriger, auf kompromittierten Rechnern durch illegal ausgestellte Zertifikate scheinbar sichere Webdienste z.B. zum Einsatz als Phishing-Webseite einzusetzen.

Revision #2
Created 25 January 2024 10:17:57 by Tina Strauf
Updated 24 April 2024 09:39:16 by Carolin Thiele