Wann hilft DNSSEC nicht?

DNSSEC wirkt lediglich auf Basis des DNS und sichert nicht die der DNS-Anfrage vorausgehenden und darauf folgenden Kommunikationsschritte ab. Es werden z.B. keine Vertipper bei der Eingabe von Domainnamen verhindert, was ein hohes Risiko darstellt. Auch wird nach der DNS Namensauflösung nicht der Verbindungsaufbau mit der via DNS erhaltenen IP-Adresse gesichert oder verifiziert (fehlerhaftes Routing/absichtliches Manipulieren von Routen kann weiterhin zu einem falschen Webserver führen), es wird nicht sichergestellt, dass die Daten der Kommunikation mit der erhaltenen IP-Adresse geschützt werden (Aufgabe von SSL).

Randbemerkung: Es kann allerdings im DNS die Signatur des SSL-Zertifikats abgelegt werden. Wenn diese Information wiederum DNSSEC signiert ist, lässt sich beim Empfänger sicherstellen, dass der korrekte Webserver kontaktiert wurde und das dort verwendete SSL-Zertifikat gültig und korrekt ist.

DNSSEC ist also kein "Rumdum-Sicher-Paket" was die Kommunikation im Internet angeht, sondern trägt lediglich im Bereich DNS einen Teil dazu bei.

Eindeutige ID: #1003
Verfasser: Thomas Klute
Letzte Änderung: 2010-04-29 11:37