

DNS Security Extensions (DNSSEC)

Sichere Verknüpfung von Internetadresse und Serveradresse





Stand: 21.01.2023, BETA

Management Summary

Mittels Signaturen wird die Verknüpfung zwischen Internetadresse (Domain) und Serveradresse (IP) gegen Fälschung geschützt. Dies verhindert eine Umlenkung von Bürgerinnen und Bürger auf Serveradressen der Angreifenden.

Ressourcenabschätzung

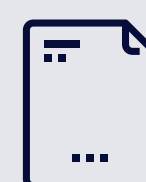
-  Mittel (50 PT)
-  Ohne neue Hardware

Erläuterung für OZG-Dienstverantwortliche

Das Domain Name System (DNS) verknüpft Internetadressen (Domain) und Serveradressen (IP) vergleichbar einem Telefonbuch. Mittels der DNS-Sicherheitserweiterungen (DNSSEC) wird diese Verknüpfung digital signiert. Dadurch werden Manipulationen erkennbar und Bürgerinnen und Bürger effektiv geschützt. DNSSEC stellt darüber hinaus eine Infrastruktur zur signierten Ab-

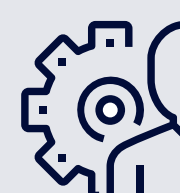
lage weiterer Informationen bereit, über die viele weitere Sicherheitstechniken realisiert werden können.

Referenz



BSI APP.3.6.A17
BSI-CS 121

Umsetzung



RZ-Betrieb oder/und
Registrar

Technischer Umsetzungsansatz

Werden die autoritativen Nameserver in externer Verantwortung, beispielsweise durch den Registrar, betrieben, reicht in der Regel eine Aktivierung im Konfigurationsmenü aus. DNSSEC ist hier zunehmend verbreitet, nur meist nicht standardmäßig aktiviert. Aufgrund des weltweit verteilten DNS-Systems dauert die Umsetzung dann wenige Stunden bis Tage.

Sofern die autoritativen Nameserver in eigener Verantwortung betrieben werden, ist auf diesen DNSSEC zu konfigurieren. Alle marktüblichen Nameserver unterstützen DNSSEC. Existiert ein Primary oder Hidden-Primary findet die Signatur der Zone dort statt, nur die signierte Zone wird an die Secondaries transferiert, das private Schlüssel-

material verbleibt auf dem Primary. Zu beachten ist, dass die Signaturen teilweise mit Ablaufzeiten versehen sind und daher ein wiederkehrender Rollover nötig ist.

Neben der Konfiguration ist die Erzeugung einiger Schlüsselpaare notwendig. Abschließend ist die Eintragung des DS-Records in der direkt über der Domain liegenden Zone (z.B. .de) nötig. Dies ist in der Regel über das Webinterface des Registrars möglich.



Da kleine Fehlkonfigurationen in diesem Bereich zur Nichterreichbarkeit aller Services in der Zone führen können, ist eine vorherige Schulung der Umsetzenden dringend geboten!