

# DNS Security Extensions (DNSSEC)

Sichere Verknüpfung von Internetadresse und Serveradresse

OZG-Security-Challenge 2023

Stand: 26.01.2023 BETA

## Management Summary



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

### Ressourcenabschätzung



Gering (<5 PT)



Ohne neue Hardware

## Erläuterung für Onlinedienst-Verantwortliche

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

### Referenz



Mittel (50 PT)

### Umsetzung



RZ-Betrieb

## 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 Schlüsselmateriale 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!**



Bundesministerium  
des Innern  
und für Heimat

Bundesamt  
für Sicherheit in der  
Informationstechnik

