

DNS und (o)TLD

- [oTLD für interne Dienste](#)

oTLD für interne Dienste

Im öffentlichen DNS Provider:

- a-Record zum internen Proxy

im internen Reverse Proxy:

- TLS Terminierung machen
- Loadbalancing machen
- kann intern erreichbar sein um internes DNS zu ermöglichen

Allgemeine Infos zum Thema:

- DMZ benutzen
- Hypervisor getrennt für intern und DMZ betreiben, nicht alles auf 1 Hypervisor betreiben
- möglichst wenige interne IP Adresse bei öffentliche DNS Providern hinterlegen
- Namen in öffentliche DNS Providern benutzen, die nicht auf die eingesetzte Software hinweisen -> Exploits direkt nutzbar
- split DNS könnte genutzt werden
 - DNS intern löst oTLD intern auf (LAN)
 - DNS extern löst oTLD extern auf (Internet)
- DNSSEC
 - kryptografische Signaturen auf DNS Einträge
 - es wird alles signiert
 - Subzonen können dann delegiert werden
 - DNSSEC geht nicht mit split DNS
- 2 getrennte oTLD für extern und intern
 - man kann DNSSEC machen
 - Nachteil doppelte Kosten
 -
- domain offensive.de -> <https://do.de>
-