



# DNS Security Strategy

---

N3K Expert Webinar Series

**Andreas Taudte**  
Principal DDI Consultant

Last updated April 2023

# Housekeeping

---

- Timing, Schedule, Q&A Session
- Online Etiquette (microphones, distracting activities)
- Recording and Privacy



# DNS Building Blocks

---



- **Platform** (hardware, operating system) of the Name Server or Resolver
- **Software** of the Name Server or Resolver
- **Transactions** (query/response, transfers, dynamic updates, notifications)
- **Database** (zone files, journal files)
- **Configuration** (named.conf, include files)

# Disaster and Human Error Defences

---

- **Geographic Provisioning** of Services against natural & unnatural Disasters (earthquakes, hurricanes, floods, terrorist attacks, acts of war)
- Periodic **User Trainings** & Communication
- **Roles & Responsibilities** clearly enumerated and understood
- **Change Control** Meetings among relevant Stakeholders
- IP Address Management System to **identify & correct potential Config. Errors**
- **Audit Logging** to enable Review



# Hardware and Operating System

---

- **Physical Access** (unplug, disconnect, console access)
- **Updates & Patches** for known Vulnerabilities (OS & service)
- Protect **Control Channel** from unauthorized Access
- **Permissions** to Servers, Directories & Files containing Service Configuration
- **Monitoring** of Logs (OS & service)

# DNS Monitoring

---

- Monitoring of the **Service** itself  
(status, version, patch level, connectivity, probe, transfer, etc.)
- **Query Logging** on caching Layers into SIEM<sup>1</sup> System incl. ECS<sup>2</sup>  
(further investigation of single and groups of DNS queries)
- Monitoring of **critical internal Records** and Systems  
(databases, call servers or internal certificate authority, etc.)
- Monitoring of **critical public Records** and Systems  
(web servers, mail exchange servers, delegations in parent zone, etc.)

<sup>1</sup> Security Information and Event Management  
<sup>2</sup> EDNS Client Subnet

# Reducing the Attack Surface

---

- Different **DNS Roles** can be attacked differently  
(authoritative DNS, caching DNS, internal or public-facing DNS)
  - **Authoritative Servers** perform resource-consuming Tasks like **dynamic Updates** or **Zone Transfers**
  - **Caching Servers** handle **Queries** from Clients and get other Servers involved for **Recursion**
- Multiple Roles provided by the same Server means bigger **Attack Surface**
- Systems with **separated Roles** can be installed and managed in **isolated Security Areas**
- Role-specific **Updates and Patches** address different Behaviours

# Internal and public-facing Caching Layer

---

- **Internal** Caching DNS
  - Configured as **Stealth Secondary** for faster Resolution
  - Subscription to **Security Feed** (known as DNS firewall)
  - Dedicated caching Layer “close” to **Clients** in remote Locations
- **External** Caching DNS
  - Performs **Internet Name Resolution**
  - Only accept **Queries from internal** Caching Servers



# Public DNS Diversity

---



- Provisioning **multiple** Servers in different **geographic Locations**
- Running a **Variety of** Server Vendor **Implementations**
- Using **multiple** external Hosting **Providers**

# DNS Role-specific Defences

---

## Stub Resolver

- **Host Controls** incl. physical, Operating Systems and Resolver Software
- DHCP Server **Audits**
- Connection **Encryption** (DoT, DoH, DoQ, etc.)

<sup>1</sup> DNS-over-TLS  
<sup>2</sup> DNS-over-HTTPS  
<sup>3</sup> DNS-over-QUIC

# DNS Role-specific Defences



## Recursive Server

- Planned **Deployment** (size, number & capacity of servers)
- **Host Controls** incl. physical, Operating Systems and Resolver Software
- **Anycast** Addressing
- Network Interface and DNS Software **ACLs**<sup>1</sup>
- **Randomization** (source port, transaction ID, query case)
- Limit Queries per Client (**rate limiting**)
- DNS Firewall (**RPZ**), **DNSSEC** Validation, **Query Log** Auditing (tunnel & malware detection)
- Connection **Encryption** (DoT, DoH, DoQ, etc.)

<sup>1</sup> Access Control List

# DNS Role-specific Defences

---

## Authoritative Server

- Planned **Deployment** (size, number & capacity of servers)
- External DNS **Service Provider** (Backup or Diversity)
- **Host Controls** incl. physical, Operating Systems and Resolver Software
- **Anycast** Addressing
- **Disable Recursion**
- Restricted **Zone Updates** and **Zone Transfers**
- **Deployment-based** Network Interface and DNS Software **ACLs** (internal, external, public-facing)
- Signing of mission-critical Zones (**DNSSEC**)

# DNS Role-specific Defences

---



## Hosting Provider

- Encrypted and unique User Access with Multi-Factor Authentication
- Integrity of every DNS Record (change history)
- DNSSEC Signing with planned and Emergency Key Rollover
- Support for other Security Features (ACLs, GeoDNS, Rate Limiting, DMARC<sup>1</sup> policy etc.)
- Service-Level Agreement (SLA)
- Denial of Service (DoS) Mitigation
- Parent Domain Security Controls

<sup>1</sup> Domain-based Message Authentication, Reporting and Conformance

# Securing each Layer of DNS

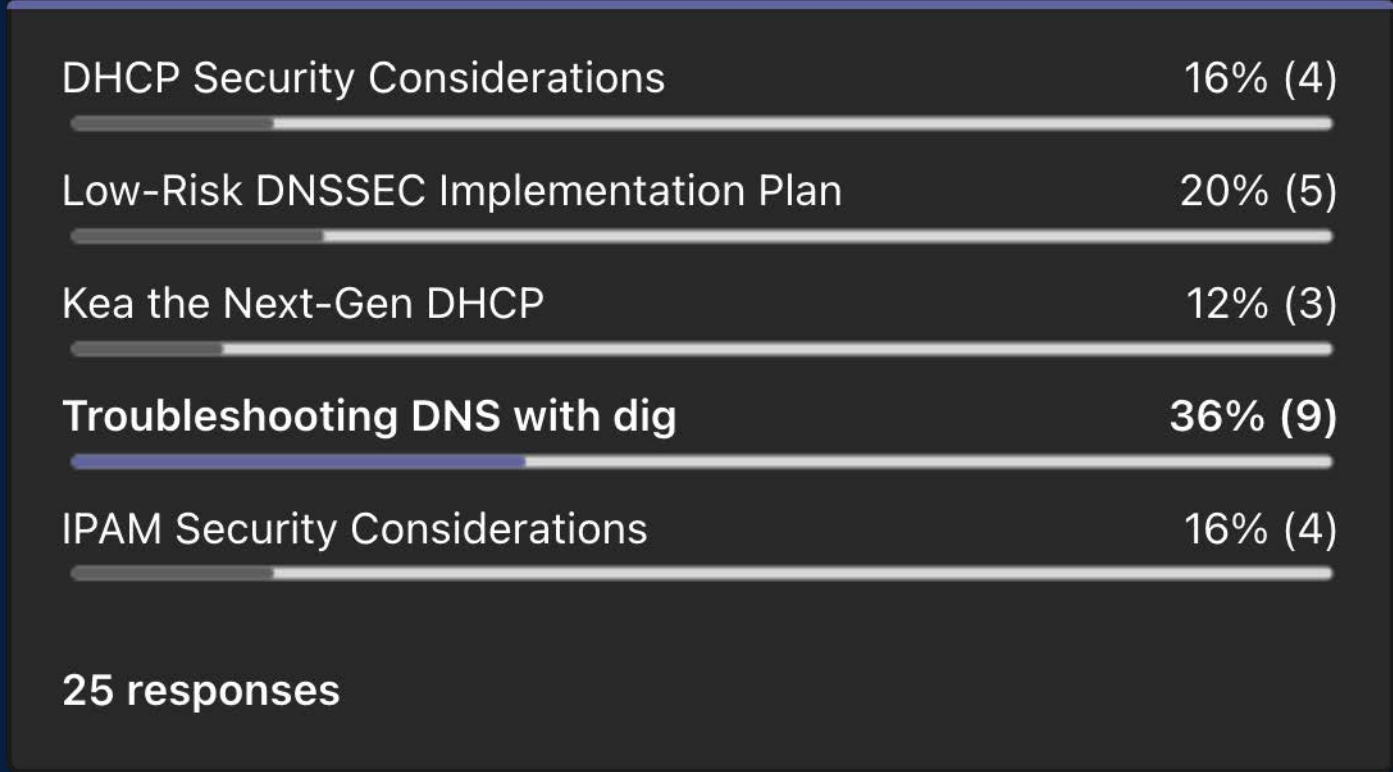


Transit Path	Transit Endpoints	Key Security Mechanisms
Recursive Query	Stub Resolver Recursive Server	ACLs, DoT, DoH, DoQ, DNSSEC
Iterative Query	Recursive Server Authoritative Server	DNSSEC
Dynamic Update	IPAM System DHCP Server/Client Authoritative Server	ACLs, Transaction Signatures (TSIG)
Zone Transfer	Primary Server Secondary Server	ACLs, TSIG
DNS Configuration	IPAM System File Editor Transfer to/from Server	SSH, SCP, SFTP, TLS




# What's next?


---



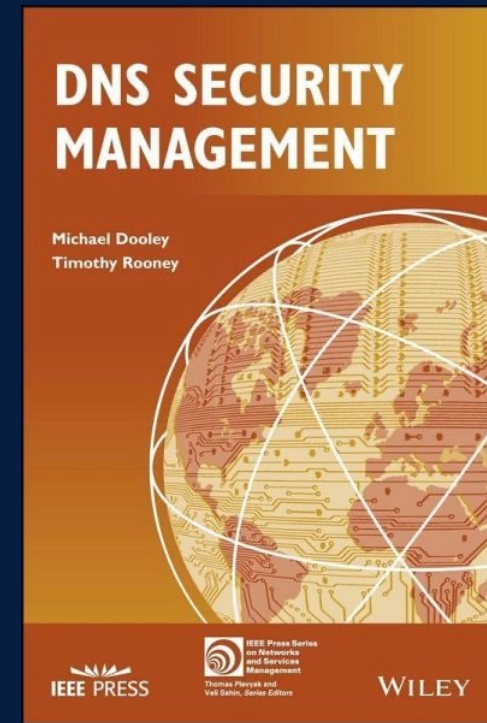
# Greedy for more?



**Enhanced  
DNS / DHCP Course  
with Mr. DDI**



https://ddiug.de  
1 0 1 0 1 0 1 0 0 0 1 0 0 1 0 0  
0 1 0 1 0 1 1 1 1 1 1 1 0 0 1 1  
1 0 1 0 1 0 0 0 0 D 1 0 1 1 0 0  
0 0 1 0 0 1 1 1 H 0 1 0 0 1  
0 1 0 1 0 0 1 C 0 0 1 1  
1 0 0 1 0 P 1 1 0 0  
1 1 0 D I 0 1  
0 0 1 N P 1 0  
0 0 S A 0  
1 M



<https://www.n3k.com/aktuelles/webinare/schulungen>  
<https://www.wiley.com/en-us/DNS+Security+Management-p-9781119331407>





# Thank you for your Time.



N3K Network Systems  
Ferdinand-Braun-Straße 2/1 | 74074 Heilbronn  
+49 7131 594 95 0  
info@n3k.de