DNS OPERATIONAL EXCELLENCE -
A RISK-BASED APPROACH AT A GLIMPSE

APTLD 76 – September 2019 – Dr. Joerg Schweiger
## DENIC – ESSENTIALS

**MANAGER OF GERMANY’S NAMESPACE .DE ON THE INTERNET**

<table>
<thead>
<tr>
<th>Neutral &amp; Non-Discriminating</th>
<th>Not-for-Profit Cooperative</th>
<th>Domain Distribution</th>
<th>Active Involved in National &amp; International Internet-Related Bodies</th>
</tr>
</thead>
<tbody>
<tr>
<td>293 Cooperative Members, 25% Non-German</td>
<td>Government-Independent &amp; Non-Regulated</td>
<td>Domain Distribution: 66% Companies, 31% Individuals, 3% Organisations</td>
<td>Management of Technical Infrastructure for DNS Anycast Services: 8.3 M DUM of Other Namespaces</td>
</tr>
</tbody>
</table>

|----------------------------------------|----------------------------------------------------------------------------------------|-----------------------|------------------|

### Domain Holders
- 7.8 M Domain Holders
- 10 Years Average Domain Lifetime
- 1.1 M Domains with International Holder

### DNS Operational Excellence - A risk-based approach
- Government-Independent & Non-Regulated
- Neutral & Non-Discriminating
- Not-for-Profit Cooperative
- Active Involved in National & International Internet-Related Bodies
- Management of Technical Infrastructure for DNS Anycast Services: 8.3 M DUM of Other Namespaces

### Domain Distribution
- 66% Companies
- 31% Individuals
- 3% Organisations

### Name Server Locations Run by DENIC Worldwide
- 18

### Data as of 31 December 2018

---

*Joerg Schweiger*
How do we deal with the ever changing threat situation?

- different, even combined types of attacks
- attacks of extreme high volume, seemingly increasing by the day
- the ease of available technology and potent devices

*holistic approach*
DENIC´S HOLISTIC RISK-BASED APPROACH

• implementation and certification of internationally recognized industry security standards in a full scope approach.
  • ISO/IEC 27001 Information Security Management System
  • ISO 22301 Business Continuity Management System

• leveraging standards as a guiding and comprehensive blueprint to design and implement DENIC-specific information security processes *and* their respective transition into operational security

• specifically for DNS we (additionally) conduct threat modeling to identify risks, which in turn lead to both proactive technical and organisational measures

• check effectiveness by simulations, drill exercises and disaster recovery tests

continuously adapt processes and operational security
HOW DOES THIS EVOLVE IN PRACTICE (SOME EXAMPLES)

• (massive) capacity upgrade (connectivity and computing)
• implementation of new network concepts for the interconnection of DENIC’s name server locations
• implementation of a distributed and pre-provisioned system environment
• threshold monitoring and automatic alarming
• leveraging secondary name service providers
To achieve excellence in operating DNS existing security management standards can be used as a systematic blueprint.

The above standards effectively direct the implementation of enterprise-specific security management processes whereas processes need to be accompanied by implementations on an operational level.

Both, processes and technical implementations need to be challenged regularly and adapted according to changing requirements.
DENIC – OUR MISSION

• DENIC sets standards for ccTLD management

• DENIC fulfils its cooperative and societal mission

• DENIC builds and shapes
  • a company that is innovative and agile as well as attractive and challenging for its staff
  • new services that are built on its core competencies
  • technologies and policies in the domain ecosystem and actively promotes a free, open and secure Internet.
ANY QUESTIONS?

CONTACT:
schweiger@denic.de

THANK YOU!