Federal Office
for Information Security

Best practice documents from BSI
… sort of

What?

not exactly BCOP document

more like security recommendations

which are kind of like BCOP

Why?

operators do things differently

document current practices of some ISPs

guidance to other ISPs

Who?

written by BSI

incorporated feedback from operators

discussed at meetings with German ISPs

So far

1. Inter-domain routing
2. DNS operators
3. DNS registrars
4. E-mail
5. Webhosting
6. DDoS reflection attacks
7. DDoS
8. IPv6
9. Malware
10. Organisational aspects

https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/ISP-Empfehlung/Internet-Service-Provider_node.html

IDR

- Protect TCP session
- Authentication
  - TCP-MD5 (TCP-AO if available)
  - GTSM
- Graceful restart
- Ingress / egress filtering
- Max prefix length
- RPKI
- RFD (if … then …)
- Limits on
  - #AS
  - AS path prepending
  - #communities
  - #prefixes
- uRPF

Malware

- Awareness
- Information on how to secure clients (available from BSI)
- AV-Bundle (if applicable)
- Support (Anti botnet initiative, ABBZ)
- Spamtraps / Honeypots
- Exchange with other ISPs
- Anti-Spoofing
- Walled garden (if necessary)

Way forward

Useful?

Which ones?

Who?

Federal Office
for Information Security