CYTAD

Complete DNS Security Checklist

FOLLOW

1.Is DNSSEC (Domain Name System Security Extensions) implemented for your domains?

☐ Yes ☐ No ☐ N/A

Remarks :

2.Do you restrict recursive DNS queries to trusted clients only?

☐ Yes ☐ No ☐ N/A

Remarks :

3.Are your DNS servers and resolvers regularly updated with security patches?

☐ Yes ☐ No ☐ N/A

Remarks :

4. Is DNS traffic encrypted using DNS over HTTPS (DoH) or DNS over TLS (DoT)

☐ Yes ☐ No ☐ N/A

Remarks :

5. Do you use DNS Response Rate Limiting (RRL) to protect against amplification attacks

☐ Yes ☐ No ☐ N/A

Remarks :

6. Is DNS server logging enabled for analyzing and monitoring DNS traffic?

☐ Yes ☐ No ☐ N/A

Remarks :

7. Are open recursive DNS servers disabled to prevent abuse?

☐ Yes ☐ No ☐ N/A

Remarks :

8. Have you configured proper DNS server access controls and firewalls?

☐ Yes ☐ No ☐ N/A

Remarks :

9. Is your DNS server protected against cache poisoning attacks?

☐ Yes ☐ No ☐ N/A

Remarks :

10. Do you regularly review and update DNS cache security mechanisms?

☐ Yes ☐ No ☐ N/A

Remarks :

11. Are you using DNS firewall or RPZ (Response Policy Zone) to block malicious domains?

☐ Yes ☐ No ☐ N/A

Remarks :

12. Do you validate DNS queries and responses to ensure their authenticity?

☐ Yes ☐ No ☐ N/A

Remarks :

13. Are you using DNS monitoring tools to detect abnormal DNS traffic patterns?

☐ Yes ☐ No ☐ N/A

Remarks :

14. Have you implemented intrusion detection systems (IDS) for DNS-based attacks?

☐ Yes ☐ No ☐ N/A

Remarks :

15. Are you monitoring DNS logs for signs of DNS tunneling and exfiltration?

☐ Yes ☐ No ☐ N/A

Remarks :

16. Do you have a procedure for responding to DNS security incidents?

☐ Yes ☐ No ☐ N/A

Remarks :

17. Do you have documented DNS security policies and procedures in place?

☐ Yes ☐ No ☐ N/A

Remarks :

18. Have your staff received DNS security training and awareness programs?

☐ Yes ☐ No ☐ N/A

Remarks :

19. Do you conduct regular security audits and assessments of your DNS infrastructure?

☐ Yes ☐ No ☐ N/A

Remarks :

20. Are DNS security roles and responsibilities clearly defined within your organization?

☐ Yes ☐ No ☐ N/A

Remarks :

21. Do you use a reputable third-party DNS filtering service to block malicious domains?

☐ Yes ☐ No ☐ N/A

Remarks :

22. Have you reviewed and vetted the security practices of your third-party DNS service provider?

☐ Yes ☐ No ☐ N/A

Remarks :

23. Do you have an incident response plan specifically tailored for DNS security incidents?

☐ Yes ☐ No ☐ N/A

Remarks :

24. Have you conducted tabletop exercises to test your DNS security incident response plan?

☐ Yes ☐ No ☐ N/A

Remarks :

25. Is there a designated team responsible for responding to DNS security incidents?

☐ Yes ☐ No ☐ N/A

Remarks :

26. Have you established communication protocols with DNS registrars and authorities for incident resolution?

☐ Yes ☐ No ☐ N/A

Remarks :

27. Are you compliant with relevant DNS security standards and regulations?

☐ Yes ☐ No ☐ N/A

Remarks :

28. Do you maintain comprehensive documentation of your DNS security measures and configurations?

☐ Yes ☐ No ☐ N/A

Remarks :

29. Do you have a DNS disaster recovery plan in place?

☐ Yes ☐ No ☐ N/A

Remarks :

30. Is your DNS infrastructure designed for redundancy and high availability?

☐ Yes ☐ No ☐ N/A

Remarks :

31. Are you prepared to adapt to emerging DNS security threats and trends?

☐ Yes ☐ No ☐ N/A

Remarks :

32. Do you actively track and assess new DNS vulnerabilities and attack vectors?

☐ Yes ☐ No ☐ N/A

Remarks :

Follow CYTAD on Linkedin for security advisories, checklists, mentoring, services, insights and much more

CYber Thinkers Advisors Doers

CYTAD - WA Channel