UMA ANALISE DO PROTOCOLO DNS E SUAS EXTENSÕES

Paulo Renato Lopes Seixas

INTRODUÇÃO

O Sistema de Nomes de Domínio(DNS) é essencial para a funcionalidade da internet, permitindo a conversão de nomes de domínio em endereços IP. Essa tradução facilita a navegação e o acesso aos recursos online. No entanto, o DNS possui vulnerabilidades que podem ser exploradas por atacantes, comprometendo a segurança das comunicações na internet.

Para combater essas ameaças, foram desenvolvidas extensões como DNSSEC e o DNSCurve, onde o DNSSEC garante autenticidade enquanto que o DNSCurve adiciona criptografia à consultas e respostas, assegurando a confidencialidade dos dados.

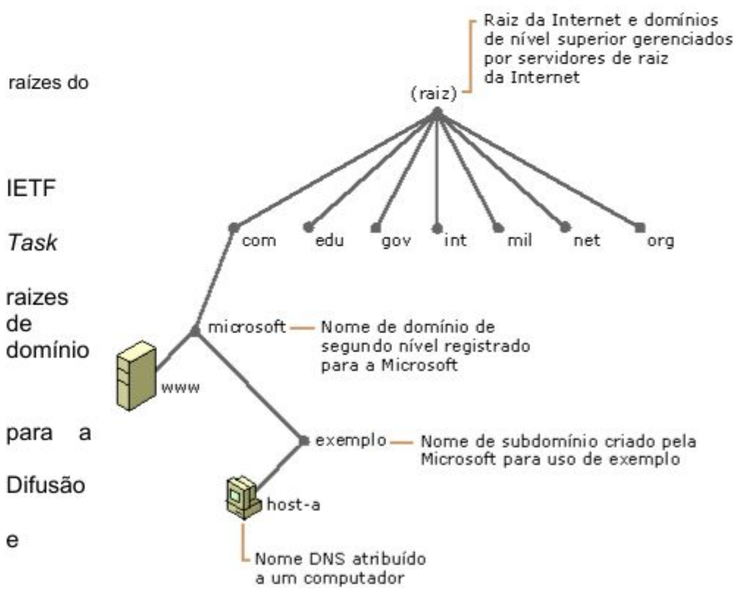

Figura 1. Hierarquia dos servidores DNS

METODOLOGIA

A metodologia de pesquisa para a análise do protocolo DNS e suas extensões doe segurança envolveu uma abrangente revisão da literatura técnica sobre o assunto. Foram coletados informações a partir de documentos fundamentais como as RFCs, além de livros e artigos de especialistas na área de redes de computadores.

Foram realizados uma análise detalhada em relação aos aspectos do histórico e fundamentos do DNS, vulnerabilidades do DNS Nativo e das extensões de segurança do DNS

OBJETIVOS

A motivação central do trabalho foi demonstrar como a implementação dessas extensões pode tornar as aplicações baseadas em DNS mais seguras, contribuindo para um ambiente de internet mais confiável e protegido contra ataques cibernéticos

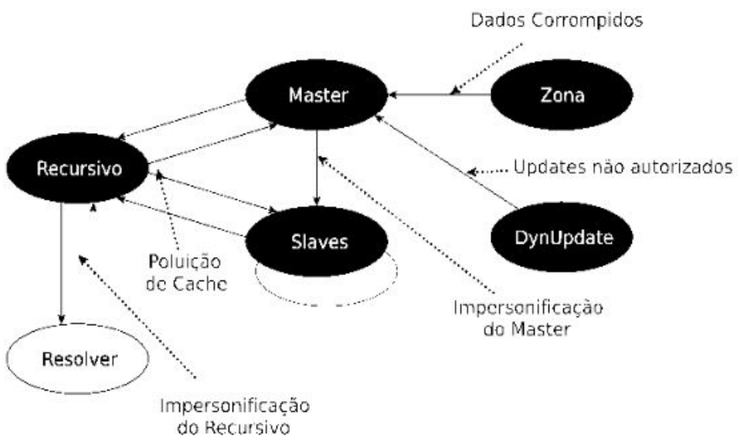

Figura 2. Vulnerabilidades no sistema de nomes de domínio

FUNDAMENTAÇÃO TEÓRICA

A fundamentação teórica deste estudo baseia-se na análise e compreensão detalhada do Sistema de Nomes de Domínio (DNS) e suas extensões de segurança, como DNSSEC e DNSCurve.

O DNS (Domain Name System) é essencial para o funcionamento da internet, pois realiza a tradução de nomes de domínio para endereços IP, permitindo que usuários acessem recursos online de maneira intuitiva.

Apesar de sua importância, o DNS nativo possui diversas vulnerabilidades, como envenenamento de cache e ataques man-in-the-middle, que podem comprometer a integridade e a confiabilidade das respostas DNS. Estas falhas intrínsecas motivaram a criação de extensões de segurança para mitigar os riscos associados.

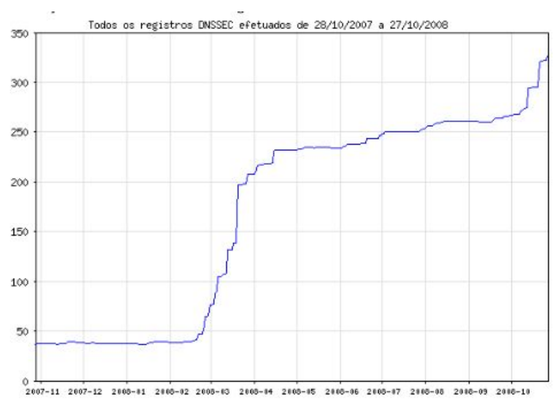

Figura 3. Registros DNSSEC efetuados no Brasul

DISCUSSÃO E RESULTADOS

Os resultados destacam que, apesar da adoção gradual do DNSSEC em domínios de primeiro nível no Brasil, ainda há desafios a serem superados. Domínios como .com.br e .gov.br ainda não implementaram completamente o DNSSEC devido a questões de vulnerabilidade na varredura de zona. No entanto, a implementação do DNSSEC em outros domínios como .eti.br, .eng.br, .adm.br e .adv.br está em progresso, o que representa um passo significativo para a melhoria da segurança do DNS no país.

Por outro lado, a adoção do DNSCurve é menos prevalente, principalmente devido ao maior consumo de dados causado pela criptografia completa dos pacotes DNS. Isso sugere que, enquanto o DNSSEC está se tornando um padrão de segurança necessário, o DNSCurve ainda enfrenta barreiras para uma implementação mais ampla.

REFERÊNCIAS

ALBITZ, Paul.; LIU, Cricket. DNS and BIND. 5th Edition. United States of América: O'Reilly Media, 2006.

TANENBAUM, Andrew S. Redes de Computadores. Tradução Vandenberg D. de Souza. 4. ed. Campus, 2003

INEMETH, Evi.; SNYDER,Garth.;HEIN,Trent R. Manual Completo do DNS. Tradução Ariovaldo Griesi. Revisão técnica Mario Olimpio de Menezes.São Paulo: Pearson Makron Books, 2004.

COSTA, Daniel G. DNS: Um guia para administradores de Redes. Rio de Janeiro: Brasport, 2006.