UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

VALMOR ANTONIO ALVES MOREIRA

DNSSEC: GARANTINDO A SEGURANÇA DO SISTEMA DE NOMES DE DOMÍNIO

GUARAPUAVA

2024

VALMOR ANTONIO ALVES MOREIRA

DNSSEC: GARANTINDO A SEGURANÇA DO SISTEMA DE NOMES DE DOMÍNIO

DNSSEC: Securing the Domain Name System

Proposta de Trabalho de Conclusão de Curso de Graduação apresentado como requisito para obtenção do título de Tecnólogo em Tecnologia em Sistemas para Internet do Curso Superior de Tecnologia em Sistemas para Internet da Universidade Tecnológica Federal do Paraná.

Orientador: Prof. Dr. Hermano Pereira

Coorientador: Prof. Dr. Luciano Ogiboski

GUARAPUAVA

2024

4.0 Internacional

Esta licença permite compartilhamento, remixe, adaptação e criação a partir do trabalho, mesmo para fins comerciais, desde que sejam atribuídos créditos ao(s) autor(es). Conteúdos elaborados por terceiros, citados e referenciados nesta obra não são cobertos pela licença.

LISTA DE ABREVIATURAS E SIGLAS

Siglas

DNS	Sistema de Nomes de Domínio
DNSSec	Extensões de Segurança do DNS
IP	Protocolo de Internet
TCP	Protocolo de Controle de Transmissão

SUMÁRIO

1 INTRODUÇÃO

A Seção de Introdução é dedicada a fornecer uma visão geral do projeto, explicando o contexto, relevância e objetivos que serão abordados ao longo do trabalho.

1.1 Considerações iniciais

A Internet revolucionou a comunicação e a busca por informações em tempo real, tornando-se indispensável na vida moderna. No entanto, esse ambiente não é isento de riscos, com usuários mal-intencionados buscando explorar vulnerabilidades, como no servidor de nomes de domínio. O Sistema de Nomes de Domínio (DNS) é essencial ao traduzir nomes de sites em endereços IP (Protocolo de Internet (IP)). Os endereços IP são fundamentais para identificar dispositivos na Internet e facilitar a comunicação entre *hosts* e servidores *web* (VIEIRA *et al.*, 2020a). Os endereços IP são essenciais para identificar dispositivos na Internet, facilitando a comunicação entre *hosts* e servidores *web*.

Os ataques cibernéticos ao DNS representam uma ameaça à integridade e confidencialidade dos dados, podendo direcionar usuários a endereços falsos e expor informações sensíveis. Para minimizar estes ataques, foram criadas as Extensões de Segurança do DNS (DNSSec), que através de assinaturas digitais geradas por certificados da cadeia de servidores DNS, buscam minimizar grande parte das falhas de segurança do serviço, com relação à autenticação e integridade, embora não abordem diretamente à confidencialidade (VIEIRA *et al.*, 2020b).

O DNSSec desempenha um papel crucial na proteção da infraestrutura da Internet, combatendo ameaças como *spoofing*, interceptação e ataques de negação de serviço (DDoS), fortalecendo a segurança online.

1.2 Objetivos

A Seção de Objetivos é dedicada a fornecer uma visão mais específica do que será abordado no trabalho.

1.2.1 Objetivo geral

O objetivo geral deste trabalho é analisar o DNSSec como uma solução para garantir a segurança do DNS. Serão explorados os conceitos, mecanismos de funcionamento e benefícios do DNSSec, com o intuito de promover sua implementação de forma cada vez mais ampla.

1.2.2 Objetivos específicos

- Apresentar o DNSSEC e seus principais componentes.
- Detalhar os mecanismos de segurança do DNSSEC, como assinaturas digitais e autenticação.
- Analisar os benefícios da implementação do DNSSEC, como a prevenção de ataques de spoofing e phishing.
- Apresentar estudos de caso e exemplos de implementações do DNSSEC em diferentes contextos.

1.3 Justificativa

A segurança do DNS desempenha um papel fundamental na confiabilidade da *Internet*. De acordo com um estudo recente (SANTOS *et al.*, 2020), a implementação do DNSSec é essencial para proteger o DNS contra ataques, tornando-se cada vez mais crucial para garantir a segurança da informação e a proteção dos usuários online. Nesse contexto, este estudo visa aprofundar o conhecimento sobre o DNSSec, explorando seus mecanismos de funcionamento e benefícios. Dessa forma, contribui não apenas para a compreensão dos desafios, mas também das oportunidades relacionadas à segurança do DNS na era digital.

1.4 Estrutura do trabalho

O restante deste trabalho está organizado da seguinte maneira: no Capítulo 2 apresentamos um referencial teórico para sustentar o desenvolvimento dos capítulos seguintes; No Capítulo 3 apresentamos a metodologia aplicada nos estudos do DNSSec; E por fim no capítulo 4 a conclusão do trabalho e apontamos uma possível continuidade na pesquisa buscando soluções cada vez mais eficientes.

2 REFERENCIAL TEÓRICO

O DNS é um dos pilares fundamentais da Internet, permitindo a tradução de nomes de domínio em endereços IP. A segurança do DNS é uma preocupação crescente devido a ataques cibernéticos, como DNS *spoofing* e *man-in-the-middle*. A implementação do DNSSEC é essencial para garantir a autenticidade e integridade das consultas DNS, protegendo contra ameaças e garantindo a confidencialidade das transmissões (VIEIRA *et al.*, 2020a).

2.1 Protocolo DNS

O protocolo DNS foi definido em 1987 e essa longevidade explica um pouco sobre a resiliência desse serviço. Contudo, o fato de o DNS ser tão duradouro e os registros de domínio serem feitos para um longo prazo de validade, somado ao fato de haver poucas equipes de segurança com experiência no assunto e pouco administradores de DNS com experiência em segurança, criam um desafio único para garantir a segurança da infraestrutura desse serviço. Assim, se forem levadas em conta as ameaças internas e externas que uma organização enfrenta, a segurança DNS passa a ser um pesadelo em potencial para qualquer equipe.

2.2 Segurança na Internet

A segurança do DNS é fundamental para a confiabilidade da Internet. A infraestrutura do DNS é vulnerável a ataques, como *DRDoS* e *DoS*, que podem ser executados por servidores DNS abertos de terceiros ou servidores de nome autoritativos na *Internet* de maneira maliciosa para o envio de consultas falsificadas para vários servidores recursivos abertos. Além disso, a falta de atualizações está sempre presente, já que, além de algumas eventuais mudanças de zona, raramente as configurações são alterada.

2.3 Extensões de Segurança para o DNS

O DNSSec é uma extensão que fornece integridade e autenticação ao serviço. No entanto, infelizmente, não em relação à confidencialidade.

O *DNSCrypt* é um *open-source* que criptografa e autentica a comunicação entre um cliente e um servidor DNS. O *DoH* e o *DoT* são funcionalidades presentes na *Cloudfire*, que são baseadas no Protocolo de Controle de Transmissão (TCP). Essas extensões de segurança são fundamentais para proteger a infraestrutura do DNS contra ataques e garantir a confidencialidade das consultas DNS.

3 METODOLOGIA

A Seção de Metodologia é dedicada a esclarecer a forma que as informações serão coletadas e trabalhadas, assim como os estudos de artigos similares a pesquisa deste trabalho.

3.1 Perspectivas

Para atingir os objetivos propostos, este estudo utilizará uma abordagem de pesquisa qualitativa, incluindo revisão bibliográfica, análise de casos de estudo e avaliação prática da implementação do DNSSec em um ambiente controlado. Serão considerados os aspectos técnicos, operacionais e de segurança relacionados à utilização do DNSSec para proteger o DNS contra ameaças cibernéticas.

4 CONSIDERAÇÕES FINAIS

O DNSSec é uma tecnologia essencial para fortalecer a segurança da Internet, oferecendo autenticação e integridade para os dados transmitidos. No entanto, sua implementação enfrenta desafios, como a necessidade de conscientização e colaboração entre diferentes entidades. Para avançar na adoção universal do DNSSec, é fundamental promover a conscientização sobre sua importância, desenvolver soluções técnicas mais eficientes e incentivar políticas que estimulem a implementação em larga escala. A colaboração entre os atores envolvidos é fundamental para superar os desafios e construir uma internet mais segura e confiável para todos os usuários.

REFERÊNCIAS

SANTOS, L. R. d. *et al.* Análise da implantação do dnssec em domínios brasileiros. **Enigma-Journal of Information Security and Cryptography**, v. 7, n. 1, p. 77–92, 2020.

VIEIRA, M. *et al.* Enhancement of dnssec: Including confidentiality to name resolution. **Enigma-Journal of Information Security and Cryptography**, v. 7, n. 1, p. 9–10, 2020.

VIEIRA, M. *et al.* Enhancement of dnssec: Including confidentiality to name resolution. **Enigma-Journal of Information Security and Cryptography**, v. 7, n. 1, p. 1, 2020.