

Analisis Strategi Implementasi Keamanan Jaringan Menggunakan daloRADIUS dan Pi-Hole DNS Server untuk Meningkatkan Keamanan Jaringan Komputer, Studi Kasus: XYZ sebagai Perusahaan Fintech = Implementation Strategy Analysis of Network Security using daloRADIUS and Pi-hole DNS Server to enhance Computer Network Security, Case Study: XYZ as a Fintech Company

Andika Davi Yudhistira, author

Deskripsi Lengkap: <https://lib.ui.ac.id/detail?id=9999920544336&lokasi=lokal>

Abstrak

Menurut laporan tahunan oleh Badan Sandi Negara pada tahun 2023, Indonesia memiliki jumlah sumber serangan siber tertinggi, dengan lebih dari 1 juta serangan, yang telah meningkat cukup pesat dibandingkan dengan 3 tahun terakhir. Beberapa platform media online telah melaporkan insiden semacam ini selama tiga tahun terakhir. Di antara 10 institusi yang terlibat dalam insiden ini, telah dikonfirmasi bahwa 6 di antaranya adalah institusi Fintech. Faktor insiden itu beragam, termasuk kurangnya kesadaran pengguna yang mengakses situs web tidak resmi di luar situs web produksi perusahaan. Tindakan ini akhirnya terbukti merugikan perusahaan. Oleh karena itu, studi ini menyoroti pentingnya RADIUS (Remote Authentication Dial-In User Service) sebagai alat keamanan komprehensif yang berkontribusi untuk mengurangi akses tidak sah dan memperkuat pertahanan jaringan terhadap ancaman yang muncul. Penelitian ini berfokus pada XYZ, Perusahaan Fintech, menggunakannya sebagai studi kasus. Pembahasan utama dalam makalah ini berfokus pada pemanfaatan server daloRADIUS untuk menyelesaikan masalah otorisasi terkait keamanan jaringan. Pi-hole DNS Server juga digunakan dalam penelitian ini untuk memblokir akses ke situs ilegal seperti pornografi dan perjudian online. Hasil penelitian ini merupakan bukti keberhasilan kombinasi komponen server daloRADIUS, router RADIUS dan DNS Server Pi-hole dalam memblokir pengguna yang terdeteksi mengakses situs ilegal dan juga diamati terkait penggunaan sumber daya Server daloRADIUS dalam rentang penggunaan mulai dari 10 pengguna aktif hingga 300 pengguna aktif.

.....According to the annual report by the National Encryption Agency in 2023, Indonesia had the highest number of cyber-attack sources, with over 1 million attacks, which has increased quite rapidly compared to the last 3 years. Several online media platforms have reported incidents of this nature over the past three years. Among the 10 institutions implicated in the present incident, it has been confirmed that 6 of them are Fintech institutions. The incident's factors are various, including the user's lack of awareness who accessed an unofficial website outside the company's production website. This act ultimately proved to be detrimental to the company. Therefore, this study highlights the importance of RADIUS (Remote Authentication Dial-In User Service) as a comprehensive security tool that contributes to mitigating unauthorized access and strengthening network defenses against emerging threats. This research focuses on XYZ, a Fintech Company, using it as a case study. The main discussion in this paper focuses on utilizing the daloRADIUS server to resolve authorization concerns regarding network security. Pi-hole DNS Server is also used in this research to block access to illegal sites such as pornography and online gambling. The results of this research are proof of the success of a combination of daloRADIUS server components, RADIUS router and Pi-hole DNS Server in blocking users who are detected accessing illegal sites and are also observed regarding the use of daloRADIUS Server resources in a usage range ranging from 10 active users to 300

active users.