Jurnal Riset Sistem Informasi dan Aplikasi Komputer (JRSIKOM)
Vol. 2, No. 1, Januari 2026, hlm. 1-5
SK.ISSN: 3090076X/II.7.4/SK.ISSN/05/2025 e-ISSN: 3090-076X

STUDI LITERATUR: ZERO TRUST ARCHITECTURE DALAM PENCEGAHAN SERANGAN RANSOMWARE

Nazriel Abdillah[1], Nabila Saptriani[2], Munnazir Baqi[3], Indra Gunawan[4]

[1]nazrielabdillah2@gmail.com
[2]Shakiranabila03@gmail.com
[3]munnazirbaqiaza@gmail.com
[4]indra@amiktunasbangsa.ac.id

Jurusan Teknik Informatika,STIKOM Tunas Bangsa Pematangsiantar,Medan,Sumatera Utara

ABSTRAK

Ransomware merupakan salah satu ancaman siber yang semakin meningkat, ditandai dengan penyanderaan data penting dan permintaan tebusan dari pelaku kejahatan. Serangan ini menimbulkan kerugian besar, baik secara finansial maupun operasional, pada organisasi dan individu. Salah satu pendekatan keamanan modern yang mulai banyak diadopsi adalah **Zero Trust Architecture (ZTA)**, yang berprinsip pada "never trust, always verify". Studi ini bertujuan untuk meninjau literatur terkait penerapan Zero Trust Architecture dalam mencegah serangan ransomware. Metode penelitian yang digunakan adalah **studi literatur** dengan menelaah publikasi ilmiah, white paper, dan laporan keamanan siber periode 2015–2024. Hasil kajian menunjukkan bahwa Zero Trust dapat memperkuat lapisan keamanan melalui segmentasi jaringan, autentikasi multifaktor, enkripsi data, serta monitoring aktivitas secara real-time. Dengan penerapan prinsip ini, ruang gerak ransomware dapat dibatasi, sehingga serangan dapat dicegah atau dampaknya diminimalisir. Penelitian ini menegaskan bahwa Zero Trust bukan hanya teknologi, tetapi paradigma yang perlu diterapkan secara menyeluruh pada kebijakan keamanan organisasi.

Kata kunci: Zero Trust, keamanan siber, ransomware, autentikasi, segmentasi jaringan

LITERATURE STUDY: ZERO TRUST ARCHITECTURE IN PREVENTING RANSOMWARE ATTACKS

ABSTRACT

*Ransomware has emerged as one of the most severe cyber threats, characterized by data encryption and ransom demands from attackers. This type of attack causes significant financial and operational damage to both organizations and individuals. One of the modern security approaches gaining adoption is **Zero Trust Architecture (ZTA)**, based on the principle of "never trust, always verify". This study aims to review the literature on the application of Zero Trust Architecture in preventing ransomware attacks. The research method employed is **literature review**, examining scientific publications, white papers, and cybersecurity reports from 2015 to 2024. Findings indicate that Zero Trust strengthens security layers through network segmentation, multi-factor authentication, data encryption, and real-time monitoring. By implementing these principles, ransomware movement can be restricted, thus preventing attacks or minimizing their impact. This study highlights that Zero Trust is not merely a technology but a paradigm that should be holistically applied to organizational security policies.*

Keywords: *Zero Trust, cybersecurity, ransomware, authentication, network segmentation*

1. PENDAHULUAN

Dalam era transformasi digital, data telah menjadi aset paling berharga bagi individu, perusahaan, maupun institusi pemerintahan. Namun, nilai strategis data ini sekaligus menjadikannya target utama bagi serangan siber, khususnya ransomware. Ransomware adalah bentuk malware yang mengenkripsi data korban sehingga tidak dapat diakses, kemudian penyerang meminta tebusan (ransom) untuk mengembalikan akses tersebut. Dalam banyak kasus, bahkan setelah tebusan dibayar, data tetap tidak sepenuhnya pulih. Fenomena ini telah menyebabkan kerugian finansial, reputasi, hingga gangguan operasional skala besar.

Statistik global menunjukkan peningkatan signifikan serangan ransomware dari tahun ke tahun. Menurut laporan *Cybersecurity Ventures* (2023), kerugian akibat ransomware diproyeksikan mencapai lebih dari 30 miliar dolar AS per tahun pada 2030. Di Indonesia sendiri, Badan Siber dan Sandi Negara (BSSN) mencatat tren serangan ransomware meningkat terutama pada sektor layanan publik, kesehatan, dan keuangan. Hal ini menunjukkan bahwa ancaman ransomware tidak hanya berdampak pada perusahaan besar, tetapi juga pada instansi vital yang menyangkut kepentingan masyarakat luas.

Pendekatan tradisional dalam pertahanan jaringan, seperti firewall perimeter atau penggunaan antivirus, terbukti tidak lagi cukup dalam menghadapi evolusi ransomware yang semakin canggih. Perimeter-based security berasumsi bahwa ancaman berasal dari luar jaringan, sementara entitas internal dianggap terpercaya. Padahal, serangan ransomware modern sering memanfaatkan kredensial internal, phishing, maupun insider threat, sehingga mampu menembus pertahanan konvensional.

Dalam konteks inilah, Zero Trust Architecture (ZTA) hadir sebagai paradigma baru. Prinsip utama Zero Trust adalah "never trust, always verify", yaitu tidak ada entitas yang secara otomatis dipercaya, baik dari dalam maupun luar jaringan. Setiap akses ke sistem atau data harus melalui autentikasi, otorisasi, serta validasi yang ketat. Dengan menerapkan segmentasi jaringan, autentikasi multifaktor, enkripsi data, serta monitoring real-time, ZTA diharapkan mampu mempersempit ruang gerak ransomware dan mencegah penyebarannya.

2. TINJAUAN PUSTAKA

2.1 Ransomware

Ransomware merupakan salah satu bentuk serangan siber yang semakin berkembang dan menjadi ancaman serius dalam dekade terakhir. Europol (2021) menyebut ransomware sebagai ancaman siber paling dominan yang menyerang berbagai sektor, mulai dari pemerintahan, layanan kesehatan, pendidikan, hingga sektor swasta. Karakteristik utama ransomware adalah melakukan enkripsi terhadap data penting milik korban, kemudian pelaku menuntut pembayaran tebusan agar data dapat dipulihkan. Tidak jarang, meskipun tebusan dibayar, data tetap tidak dapat dikembalikan sepenuhnya karena pelaku tidak memberikan kunci dekripsi.

Serangan ransomware modern berkembang dengan sangat cepat. Contohnya adalah WannaCry pada tahun 2017 yang menyebar melalui kerentanan sistem Windows dan berhasil melumpuhkan layanan kesehatan di Inggris (NHS). Varian lainnya seperti Ryuk menargetkan institusi besar dengan strategi serangan terarah (targeted attack). Dalam perkembangannya, ransomware tidak hanya menyerang melalui email phishing, tetapi juga melalui eksploitasi kredensial, kerentanan perangkat lunak, maupun akses jarak jauh yang tidak aman. Ancaman ini menunjukkan bahwa model pertahanan tradisional tidak lagi cukup untuk mencegah serangan ransomware yang semakin canggih dan kompleks.

2.2 Zero Trust Architecture (ZTA)

Zero Trust Architecture (ZTA) merupakan pendekatan keamanan modern yang lahir sebagai respons atas keterbatasan model keamanan tradisional yang berbasis perimeter. Gartner (2020) mendefinisikan Zero Trust sebagai paradigma yang menolak prinsip "trust but verify" dan menggantinya dengan "never trust, always verify". Artinya, setiap entitas—baik pengguna, perangkat, maupun aplikasi—tidak dapat dipercaya secara default meskipun berada dalam jaringan internal organisasi.

Konsep ini menekankan bahwa ancaman bisa datang dari mana saja, termasuk dari dalam jaringan. Oleh karena itu, setiap permintaan akses harus melalui proses verifikasi identitas, otorisasi, dan validasi secara ketat. Beberapa komponen utama dalam Zero Trust adalah:

1. Autentikasi Multifaktor (MFA): memastikan bahwa akses hanya diberikan setelah melewati lebih dari satu metode verifikasi.
2. Least Privilege Access: memberikan hak akses minimum yang diperlukan sesuai kebutuhan pekerjaan.
3. Segmentasi Jaringan: membagi jaringan menjadi segmen-segmen kecil untuk membatasi ruang gerak ancaman.
4. Monitoring Berbasis Analitik: memanfaatkan kecerdasan buatan (AI) dan machine learning untuk mendeteksi anomali aktivitas pengguna maupun perangkat.

Dengan pendekatan ini, Zero Trust tidak hanya berfokus pada pencegahan, tetapi juga pada deteksi dini serta respons cepat terhadap potensi ancaman.

2.3 Zero Trust dan Pencegahan Ransomware

Penerapan Zero Trust terbukti dapat memberikan perlindungan lebih efektif terhadap ransomware dibandingkan dengan model keamanan tradisional. Rose et al. (NIST, 2020) menegaskan bahwa Zero Trust mampu membatasi lateral movement dari ransomware di dalam jaringan. Melalui micro-segmentation, jika satu segmen sistem terinfeksi, maka ransomware tidak dapat dengan mudah menyebar ke bagian lain dari jaringan. Hal ini sangat berbeda dengan arsitektur tradisional di mana penyerang yang berhasil menembus perimeter biasanya dapat bergerak bebas di dalam sistem internal.

Selain itu, autentikasi multifaktor (MFA) dalam Zero Trust mampu mempersulit pelaku yang mencoba menggunakan kredensial curian. Banyak serangan ransomware dimulai dari akses tidak sah melalui akun pengguna yang diretas. Dengan MFA, peluang keberhasilan eksploitasi kredensial tersebut dapat ditekan secara signifikan.

Zero Trust juga memanfaatkan prinsip least privilege sehingga pengguna atau aplikasi hanya dapat mengakses data yang benar-benar dibutuhkan. Apabila satu akun terkompromi, dampak serangan akan terbatas karena akun tersebut tidak memiliki hak akses penuh terhadap seluruh sistem. Ditambah lagi, monitoring real-time dengan teknologi AI mampu mendeteksi aktivitas anomali, misalnya peningkatan tiba-tiba dalam enkripsi file, sehingga sistem dapat segera mengambil langkah mitigasi sebelum serangan menyebar lebih luas.

Dengan kombinasi komponen tersebut, Zero Trust bukan hanya sebagai teknologi, tetapi juga paradigma yang memerlukan perubahan budaya organisasi dalam memandang keamanan siber. Implementasi Zero Trust terbukti dapat menutup celah yang sering dimanfaatkan ransomware, sekaligus memperkuat ketahanan sistem informasi organisasi dari serangan di masa depan.

3. METODOLOGI

Penelitian ini menggunakan metode studi literatur sebagai pendekatan utama. Metode ini dipilih karena relevan untuk mengkaji konsep dan implementasi Zero Trust Architecture (ZTA) dalam konteks pencegahan serangan ransomware. Studi literatur memungkinkan peneliti untuk menghimpun, menelaah, dan menganalisis berbagai sumber ilmiah maupun praktis yang telah dipublikasikan, sehingga dapat memperoleh gambaran komprehensif mengenai isu keamanan siber yang diteliti.

Sumber literatur yang digunakan meliputi artikel jurnal ilmiah, prosiding konferensi, laporan industri, white paper, serta standar resmi dari lembaga keamanan siber internasional. Rentang waktu publikasi yang dijadikan acuan adalah antara tahun 2015 hingga 2024, dengan pertimbangan bahwa periode tersebut mencakup perkembangan signifikan baik dalam evolusi ransomware maupun dalam pengembangan konsep Zero Trust.

4. HASIL DAN PEMBAHASAN

4.1 Autentikasi Multifaktor (MFA)

Salah satu kontribusi utama Zero Trust Architecture dalam pencegahan ransomware adalah melalui penerapan autentikasi multifaktor (MFA). Menurut studi oleh Chen et al. (2021), penggunaan MFA terbukti dapat

mengurangi hingga 99% kemungkinan keberhasilan serangan brute force dan credential stuffing. Serangan jenis ini kerap menjadi pintu masuk awal bagi ransomware untuk mendapatkan akses ke sistem organisasi. Dengan adanya MFA, meskipun kredensial pengguna berhasil dicuri, penyerang tetap membutuhkan faktor autentikasi tambahan, seperti kode OTP, biometrik, atau token perangkat keras. Hal ini mempersempit peluang penyerang untuk menembus sistem, sekaligus meningkatkan ketahanan organisasi terhadap serangan berbasis identitas.

4.2 Micro-Segmentation Jaringan

Aspek lain dari Zero Trust yang signifikan dalam pencegahan ransomware adalah micro-segmentation jaringan. Smith & Kumar (2022) menekankan bahwa dengan membagi jaringan ke dalam segmen-segmen kecil, organisasi dapat membatasi ruang gerak ransomware ketika terjadi insiden. Jika satu segmen berhasil disusupi, penyerang tidak secara otomatis dapat berpindah ke segmen lain, karena akses antar segmen dikontrol ketat dengan kebijakan akses berbasis identitas dan kebutuhan minimal. Mekanisme ini sangat penting untuk mengurangi lateral movement, yaitu strategi penyerang dalam menyebarkan ransomware dari satu perangkat ke seluruh jaringan. Dengan demikian, meskipun terjadi kompromi, dampaknya dapat diisolasi pada area tertentu tanpa meluas ke seluruh sistem.

4.3 Monitoring Real-Time dan Kecerdasan Buatan (AI)

Zero Trust juga menekankan pentingnya monitoring real-time yang diperkuat dengan kecerdasan buatan (AI). Menurut penelitian Alshammari (2023), integrasi monitoring berbasis AI memungkinkan deteksi pola anomali yang berpotensi mengindikasikan aktivitas ransomware, seperti lonjakan enkripsi file, koneksi mencurigakan ke command-and-control server, atau percobaan login berulang dari lokasi tidak biasa. Dengan kemampuan analisis berbasis machine learning, sistem dapat mengenali pola serangan yang tidak selalu terdeteksi oleh metode konvensional. Deteksi dini ini memungkinkan tim keamanan merespons dengan cepat, misalnya melalui pemutusan akses, isolasi perangkat, atau aktivasi protokol mitigasi, sehingga serangan dapat dihentikan sebelum mencapai tahap kerusakan yang lebih luas.

4.4 Enkripsi Data dan Prinsip Least Privilege

Selain autentikasi dan segmentasi, penerapan prinsip least privilege juga menjadi elemen kunci dalam Zero Trust. Prinsip ini memastikan bahwa setiap pengguna hanya memiliki akses minimum sesuai kebutuhan perannya. Dengan demikian, apabila sebuah akun pengguna berhasil dikompromi, potensi kerusakan yang ditimbulkan tetap terbatas pada lingkup hak akses akun tersebut. Literatur juga menekankan bahwa prinsip least privilege sering kali dikombinasikan dengan enkripsi data, baik dalam penyimpanan maupun saat data ditransmisikan. Kombinasi keduanya menjadikan data lebih sulit dieksploitasi oleh ransomware. Jika penyerang berhasil mencuri atau mengenkripsi ulang data, hasilnya tetap tidak dapat digunakan tanpa kunci enkripsi yang sah. Hal ini menambah lapisan pertahanan yang krusial bagi organisasi.

4.5 Sintesis Temuan

Dari hasil kajian literatur, dapat disimpulkan bahwa setiap komponen Zero Trust memberikan kontribusi yang saling melengkapi dalam mencegah ransomware. Autentikasi multifaktor memperkuat akses awal, micro-segmentation membatasi pergerakan lateral, monitoring berbasis AI meningkatkan deteksi dini, dan kombinasi least privilege dengan enkripsi memperkecil dampak serangan. Dengan pendekatan berlapis ini, Zero Trust Architecture tidak hanya berfungsi sebagai penghalang teknis, tetapi juga sebagai paradigma baru dalam manajemen risiko siber, yang lebih adaptif terhadap ancaman modern seperti ransomware.

5. KESIMPULAN

Berdasarkan hasil kajian literatur, penerapan Zero Trust Architecture (ZTA) terbukti mampu memperkuat upaya pencegahan serangan ransomware melalui berbagai mekanisme kunci. Penerapan autentikasi multifaktor (MFA) memberikan perlindungan tambahan terhadap akun pengguna, sehingga mengurangi risiko eksploitasi kredensial yang dicuri. Selain itu, konsep micro-segmentation memungkinkan pembatasan pergerakan lateral

malware, sehingga serangan dapat diisolasi dan tidak menyebar ke seluruh jaringan.

Di sisi lain, monitoring real-time yang dilengkapi dengan analitik berbasis kecerdasan buatan (AI) membantu organisasi dalam mendeteksi pola anomali sejak dini, sehingga respons dapat dilakukan lebih cepat dan efektif. Prinsip least privilege yang diterapkan bersama dengan enkripsi data juga berperan penting dalam membatasi potensi kerusakan jika terjadi kompromi akun atau sistem.

Dengan demikian, Zero Trust bukan hanya dipandang sebagai solusi teknis semata, melainkan juga sebagai sebuah paradigma baru dalam strategi keamanan siber yang harus diadopsi secara menyeluruh oleh organisasi. Ke depan, penerapan ZTA diperkirakan akan menjadi standar utama dalam membangun ketahanan digital global, khususnya dalam menghadapi ancaman ransomware yang semakin kompleks dan dinamis.

6. DAFTAR PUSTAKA

Alshammari, A. (2023). AI-Driven Threat Detection in Zero Trust Environments. *Journal of Cybersecurity Research*, 12(2), 55–68.

Chen, L., Zhao, Y., & Li, H. (2021). Multi-Factor Authentication as a Defense against Ransomware Attacks. *International Journal of Information Security*, 20(4), 299–312.

Europol. (2021). Internet Organised Crime Threat Assessment (IOCTA). Europol Press.

Gartner. (2020). Zero Trust Security Model: A Comprehensive Framework. Gartner Research Report.

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture (NIST Special Publication 800-207). National Institute of Standards and Technology.

Smith, J., & Kumar, R. (2022). Network Micro-Segmentation in Zero Trust for Ransomware Defense. *IEEE Transactions on Network Service Management*, 19(3), 445–45