JURNAL ILMIAH SAINS & TEKNOLOGI
UNIVERSITAS BANTEN JAYA

Jurnal Ilmiah Sains dan Teknologi Vol. 9, No. 1, Februari 2025
P–ISSN: 1907-1205
E-ISSN: 2622-6391

DEFENSE IN DEPTH UNTUK APLIKASI KEBUGARAN PERUSAHAAN START-UP MENGGUNAKAN MICROSOFT AZURE

Holilah[1], Husyen Ali Alhabsy[2], Tb. Muhammad Farhan Adnan[3], Voully Abdullah Zhacque[4], Royan Habibie Sukarna[5], Mohamad Hilman[6], Andi Moch Januriana[7]
Program Studi Informatika, Fakultas Teknik, Universitas Sultan Ageng Tirtayasa[1,2,3,4,5,6],
Program Studi Pertanahan, Sekolah Tinggi Pertanahan Nasional[7]
Email: [1]holilah@untirta.ac.id, 3337220007@untirta.ac.id[2], 3337220038@untirta.ac.id[3],
3337220066@untirta.ac.id[4], royan@untirta.ac.id[5], mohamad.hilman@untirta.ac.id[6],
amj@stpn.ac.id[7]

Abstract

A start-up company in the fitness and health sector has developed an innovative virtual training platform. The platform allows users to take live fitness classes via their computer, tablet or smartphone, leveraging artificial intelligence (AI) and high-quality video streaming for an interactive and personalized training experience. The platform consists of three main components: the frontend layer (web and mobile applications), the backend layer (application servers), and the data storage layer (cloud database). As the popularity of these platforms increases, companies face challenges in managing on-premises resources, ensuring data security, and complying with strict data protection regulations. This research aims to design a comprehensive cyber security strategy by utilizing Microsoft Azure services to overcome these challenges. This strategy includes identity and access management, data encryption, threat detection and response, and regulatory compliance. Using a "Seven Layer Defense in Depth" approach, this research aims to improve platform security, support rapid user growth, and ensure compliance with data protection regulations.
Keywords: *Defense in Depth, Cybersecurity, Microsoft Azure, Virtual Fitness, Data Protection.*

PENDAHULUAN

Dalam era digital saat ini banyak perusahaan start-up berbasis teknologi tergolong dalam bisnis baru dari semua startup termasuk di bidang kebugaran dan kesehatan (Ningsih et al., 2023). Kesehatan dan kebugaran telah menjadi kebutuhan penting bagi manusia oleh karena itu berbagai macam teknologi dikembangkan untuk mendukung kemudahan dalam hal kesehatan dan kebugaran(Antoni & Suharjana, 2019) dengan memanfaatkan teknologi kecerdasan buatan (AI) seorang instruktur dapat digantikan oleh sebuah aplikasi yang bisa membantu pemula atau orang awam untuk melakukan gerakan olahraga dengan tepat (Nazario Istalaksana et al., 2022), perusahaan start-up di bidang kebugaran dan kesehatan telah mengembangkan sebuah platform pelatihan virtual yang inovatif untuk memberikan solusi kesehatan yang personal, mudah diakses, dan terintegrasi dengan perangkat komputer, tablet, atau ponsel pintar mereka.

Perusahaan start-up ini menyediakan pengalaman pelatihan yang interaktif dan personal bagi setiap penggunanya yang memiliki tingkat kesibukan dalam beraktifitas sehingga mempermudah dalam suatu kegiatan(Mulyapati & Agasia, 2019). Kelas yang ditawarkan mencakup berbagai jenis latihan, mulai dari yoga, pilates, hingga latihan kekuatan dan kardio. Namun, popularitas ini juga menarik perhatian menganai ancaman keamanan siber yang dapat membahayakan data pengguna, seperti informasi kesehatan pribadi, riwayat aktivitas, dan data keuangan. Yang termasuk serangan berbahaya adalah malware, serangan berbasis web dan penolakan layanan (Yuliartanto&Soewito, 2024). Bagi perusahaan start-up yang seringkali

memiliki keterbatasan sumber daya, memastikan keamanan aplikasi menjadi tantangan yang signifikan.

Sejumlah penelitian sebelumnya telah membahas pengembangan aplikasi kebugaran dan kesehatan untuk kemudahan berolahraga. Namun, masih perlu penambahan dalam literatur terkait penerapan keamanan data dalam pengembangan aplikasi tersebut. Penggunaan Defense in Depth (DiD) di Microsoft Azure dapat membawa keuntungan yang signifikan pada perlindungan data. Penelitian ini menambahkan literatur dengan menggunakan Defense in Depth (DiD) di Microsoft Azure dalam mengatasi tantangan yang dihadapi perusahaan start-up saat ini. Microsoft Azure, adalah merupakan platform Cloud Computing publik yang dikembangkan oleh Microsoft Corporation(Sulaksono & Giovanni, 2020), selain Defense in Depth (DiD) di Microsoft Azure juga terdapat layanan Platform as a Service (Paas)(Anugerah et al., 2022).

Defense in Depth (DiD) adalah pendekatan keamanan berlapis yang menggabungkan berbagai strategi dan teknologi untuk melindungi sistem dari ancaman siber. Pendekatan ini bekerja dengan mengintegrasikan langkah-langkah perlindungan pada berbagai lapisan, mulai dari infrastruktur hingga data, sehingga menciptakan sistem yang lebih tangguh terhadap serangan. DiD sangat relevan untuk perusahaan start-up yang ingin membangun kepercayaan pengguna dan memastikan keberlanjutan bisnis mereka dalam lingkungan digital yang penuh risiko. Penerapan DiD mencakup langkah-langkah seperti pengelolaan identitas berbasis peran (RBAC), autentikasi multifaktor (MFA), enkripsi komunikasi, dan kebijakan backup otomatis. Pendekatan ini tidak hanya melindungi data sensitif pengguna, tetapi juga memastikan aplikasi tetap berfungsi secara optimal meskipun menghadapi ancaman keamanan dan bagi perusahaan start-up yang mengembangkan aplikasi kebugaran, platform ini menjadi pilihan ideal untuk mengelola infrastruktur, aplikasi, dan data secara aman dan efisien.

Penelitian ini bertujuan untuk meningkatkan keamanan aplikasi kebugaran perusahaan start-up dengan menerapkan pendekatan Defense in Depth (DiD) di microsoft azure. Melalui penerapan ini, diharapkan dapat mendukung pertumbuhan pengguna yang pesat, dan memastikan kepatuhan terhadap regulasi perlindungan data sesuai dengan kebutuhan industri.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan metode studi kasus untuk merancang strategi keamanan siber pada platform perusahaan start-up. adapun tahapan Penelitian ini diantaranya :

1. Populasi dan Sampel

Subjek penelitian ini adalah platform sebuah perusahaan start-up teknologi yang menyediakan layanan pelatihan kebugaran virtual. Sampel penelitian diambil dari tiga kelompok utama:

a. Pengguna Akhir : Pelanggan yang menggunakan platform untuk mengikuti kelas kebugaran.

b. Instruktur : Profesional kebugaran yang memberikan pelatihan melalui platform.

c. Karyawan Perusahaan : Staf yang terlibat dalam pengelolaan dan pengembangan platform.

Metode pengambilan sampel yang digunakan adalah *purposive sampling*, dimana peneliti memilih individu-individu yang dianggap memiliki informasi penting dan relevan dengan topik penelitian.

2. Instrumen dan Prosedur Pengumpulan Data

Dalam penelitian ini, pengumpulan data merupakan langkah krusial untuk memperoleh informasi yang relevan dan mendalam mengenai penerapan strategi keamanan di perusahaan. Untuk mencapai tujuan ini, beberapa instrumen dan prosedur akan digunakan untuk memastikan data yang dikumpulkan akurat dan komprehensif.

a. **Wawancara Semi-Terstruktur:** Wawancara dilakukan dengan ahli keamanan siber dan karyawan perusahaan untuk mendapatkan pemahaman mendalam mengenai tantangan keamanan yang dihadapi dan solusi yang telah diterapkan.
b. **Dokumentasi:** Analisis dokumen seperti kebijakan keamanan perusahaan, laporan insiden keamanan, dan regulasi perlindungan data yang berlaku.
c. **Observasi:** Pengamatan langsung terhadap proses pengelolaan keamanan di perusahaan untuk memahami praktik-praktik yang diterapkan.

Prosedur pengumpulan data dimulai dengan penyusunan panduan wawancara, dilanjutkan dengan pelaksanaan wawancara, pengumpulan dokumen terkait, dan observasi lapangan. Data yang diperoleh kemudian dicatat dan dianalisis secara sistematis.

3. Analisis Data

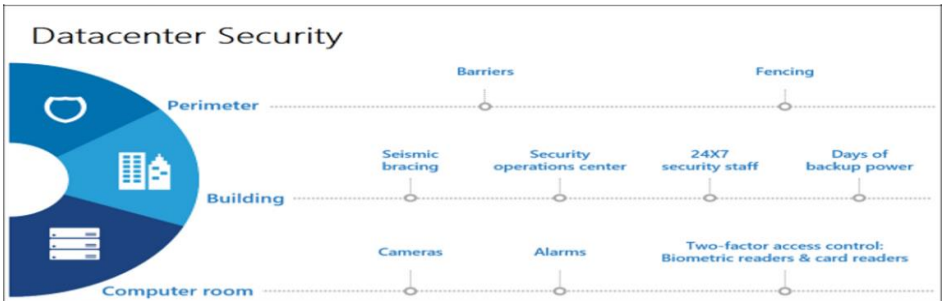
Tahap selanjutnya adalah analisis data yang bertujuan untuk mengidentifikasi pola, tema, dan wawasan yang dapat memberikan gambaran mendalam mengenai penerapan strategi keamanan siber di perusahaan. Teknik analisis yang digunakan adalah analisis tematik, yang merupakan pendekatan sistematis untuk memahami dan mengorganisasi data kualitatif. Proses analisis tematik melibatkan beberapa langkah utama sebagai berikut:

a. **Transkripsi Data:** Langkah pertama adalah mentranskrip wawancara dan mencatat hasil observasi serta dokumentasi. Proses ini memastikan bahwa semua data yang diperoleh dari wawancara, observasi, dan dokumen tersedia dalam format yang dapat dianalisis lebih lanjut.
b. **Pengkodean:** Setelah data ditranskrip, langkah berikutnya adalah mengidentifikasi dan memberi kode pada tema-tema yang muncul dari data. Pengkodean membantu dalam menandai bagian-bagian penting dari data yang relevan dengan tujuan penelitian.
c. **Kategorisasi:** Tema-tema yang telah diberi kode kemudian dikelompokkan menjadi kategori yang lebih besar. Kategorisasi ini memudahkan dalam mengorganisasi data yang serupa dan membantu dalam menyusun informasi yang terstruktur.
d. **Interpretasi:** Langkah terakhir adalah menganalisis hubungan antara kategori dan menyusun kesimpulan serta rekomendasi berdasarkan temuan penelitian. Interpretasi ini bertujuan untuk mengidentifikasi pola-pola penting dan menyusun strategi yang komprehensif berdasarkan hasil analisis.

HASIL DAN PEMBAHASAN (12pt bold)

Penelitian ini dikembangkan mengunakan Microsoft Azure dengan penerapan Defense in Depth (DiD). Defense in Depth (DiD) adalah strategi keamanan yang menggunakan pendekatan berlapis untuk melindungi sistem dan data dari berbagai ancaman. Pendekatan ini mirip dengan pertahanan abad pertengahan, di mana beberapa lapisan digunakan untuk memperlambat dan menghambat penyerang, memberikan lebih banyak waktu untuk mendeteksi dan merespons serangan. Berikut ini adalah prinsip-prinsip utama dari Defense in Depth, yang diimplementasikan secara menyeluruh dengan kebijakan dan prosedur yang sangat aman, khususnya dalam pengelolaan akses, respons serangan, dan kepatuhan terhadap peraturan:

1. **Keamanan Fisik** atau **Layer 1**: Melindungi infrastruktur fisik seperti pusat data, server, dan perangkat keras dari akses yang tidak sah dan kerusakan fisik.



Gambar 1. Keamanan Fisik

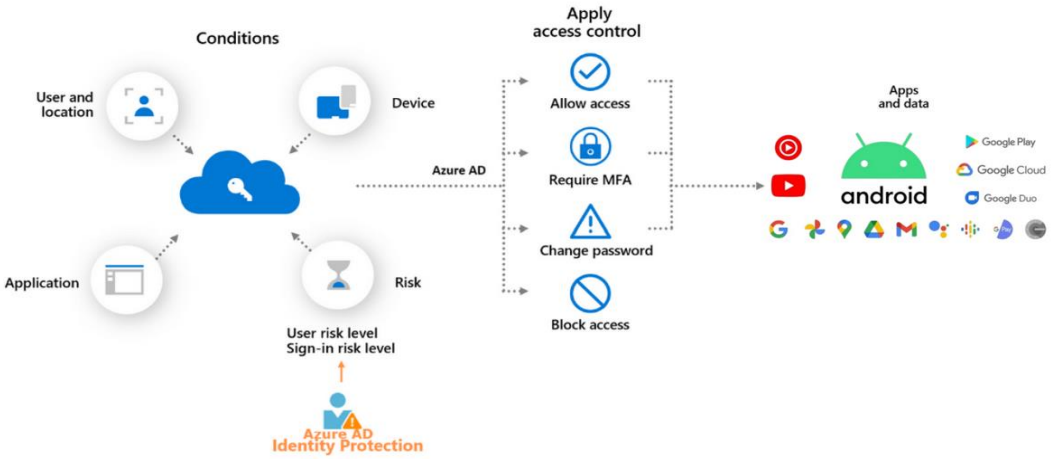
a. Perimeter dan Bangunan

1. Barriers (Penghalang): Menghalangi akses langsung ke pusat data.
2. Fencing (Pagar): Mengelilingi pusat data, sering dilengkapi sensor.
3. 24X7 Security Staff (Petugas Keamanan 24 Jam): Mengawasi dan merespons ancaman sepanjang waktu.
4. Seismic Bracing (Perkuatan Seismik): Struktur tahan gempa.
5. Security Operations Center (Pusat Operasi Keamanan): Mengelola keamanan fasilitas.
6. Days of Backup Power (Daya Cadangan): Daya cadangan untuk operasi berkelanjutan.

b. Ruang Komputer

1. Cameras (Kamera): Memantau aktivitas di seluruh pusat data.
2. Alarms (Alarm): Memberi peringatan terhadap akses yang tidak sah atau situasi darurat.
3. Two-Factor Access Control (Kontrol Akses Dua Faktor): Menggunakan biometrik dan kartu untuk memastikan hanya orang berwenang yang bisa masuk.

2. Keamanan Identitas dan Akses atau **Layer 2**: Mengelola hak akses dan autentikasi pengguna untuk memastikan hanya pengguna yang berwenang dapat mengakses sistem dan data sensitif. Kebijakan yang diterapkan memungkinkan pengelolaan yang aman dan terukur



terhadap akses, serta respons cepat terhadap ancaman akses tidak sah.

Gambar 2. Keamanan Identitas dan Akses

a. Kondisi (Conditions)

1. Pengguna dan Lokasi: Memeriksa identitas dan lokasi geografis pengguna.
2. Perangkat: Memeriksa jenis dan status keamanan perangkat yang digunakan.
3. Aplikasi: Menilai aplikasi yang diakses, berdasarkan sensitivitas data.
4. Risiko: Menilai risiko dari aktivitas dan sign-in pengguna.

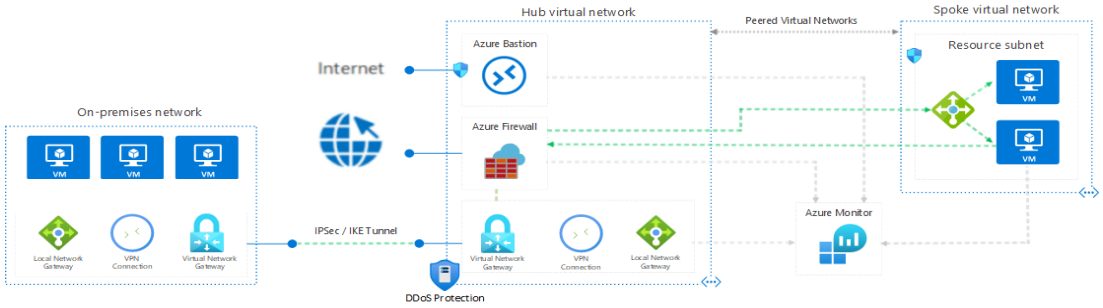
b. Azure AD Identity Protection

1. Tingkat Risiko Pengguna: Menilai kemungkinan akun pengguna telah dikompromikan.
2. Tingkat Risiko Sign-in: Menilai risiko dari setiap upaya sign-in.

c. Penerapan Kontrol Akses (Apply Access Control)

1. Izinkan Akses: Akses penuh diberikan jika aman.
2. Memerlukan MFA (Multi-Factor Authentication): Membutuhkan autentikasi tambahan jika risiko meningkat.
3. Ganti Kata Sandi: Mengharuskan perubahan kata sandi jika risiko terdeteksi.
4. Blokir Akses: Akses diblokir jika risiko terlalu tinggi.

3. Keamanan Perimeter atau **Layer 3**: Melindungi akses ke aplikasi dari luar jaringan organisasi dengan menggunakan layanan seperti gateway aplikasi dan pengendalian akses berbasis web. Implementasi kebijakan ini membantu memastikan bahwa perimeter jaringan tetap tangguh terhadap berbagai ancaman dari luar.



Gambar 3. Keamanan Perimeter

a. On-Premises Network:
1. **VM (Virtual Machines):** Server yang di-host di pusat data lokal, digunakan untuk menjalankan aplikasi dan layanan internal(Susanto et al., 2022).
2. **Local Network Gateway:** Menghubungkan jaringan on-premises ke jaringan virtual di Azure.
3. **VPN Connection:** Mengamankan koneksi antara jaringan on-premises dan Azure menggunakan protokol VPN.
4. **Virtual Network Gateway:** Menghubungkan jaringan virtual di Azure dengan jaringan on-premises melalui VPN.

b. Internet:
1. **IPSec / IKE Tunnel:** Mengamankan komunikasi antara jaringan on-premises dan Azure menggunakan protokol IPSec dan IKE untuk enkripsi.

c. Hub Virtual Network (Azure):
1. **Azure Bastion:** Memberikan akses aman ke virtual machines di Azure tanpa memerlukan IP publik.
2. **Azure Firewall:** Mengelola lalu lintas jaringan masuk dan keluar, serta menyediakan perlindungan terhadap ancaman dengan aturan firewall.
3. **Virtual Network Gateway:** Menghubungkan jaringan virtual Azure dengan jaringan on-premises melalui VPN.
4. **VPN Connection:** Koneksi VPN yang menghubungkan Azure dengan jaringan on-premises.
5. **Local Network Gateway:** Menghubungkan jaringan virtual di Azure dengan jaringan on-premises.

d. DDoS Protection:
1. Memberikan perlindungan terhadap serangan Distributed Denial of Service (DDoS) untuk menjaga ketersediaan dan performa layanan.

e. Spoke Virtual Network (Azure):
1. **Resource Subnet:** Subnet dalam jaringan virtual yang menampung resource seperti virtual machines.
2. **VM (Virtual Machines):** Server yang di-host di Azure, digunakan untuk menjalankan aplikasi dan layanan.
3. **Local Network Gateway:** Menghubungkan subnet resource ke hub virtual network di Azure.

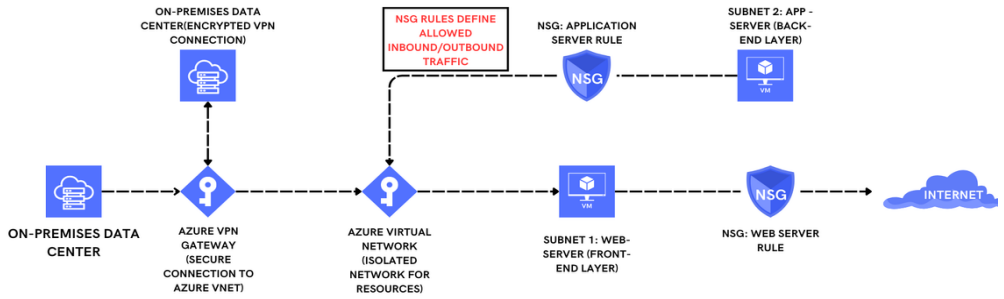
f. Peered Virtual Networks:

1. Menghubungkan beberapa jaringan virtual di Azure untuk memungkinkan komunikasi antar resource dalam berbagai jaringan virtual.

g. Azure Monitor:

1. Layanan untuk memantau performa, diagnostik, dan keamanan jaringan serta resource di Azure.

4. Keamanan Jaringan atau **Layer 4**: Melibatkan perlindungan jaringan komputer dari akses yang tidak sah, serangan cyber, dan ancaman lainnya melalui pengaturan firewall, mitigasi serangan DDoS, dan segmentasi jaringan. Implementasi prosedur ini menekankan pada penggunaan teknologi canggih untuk memastikan keamanan jaringan yang tangguh.



Gambar 4. Keamanan Jaringan

a. Azure VPN Gateway:

1. Azure VPN Gateway menyediakan konektivitas terenkripsi antara pusat data on-premises dan Azure Virtual Network (VNet). Ini memastikan bahwa semua data yang dikirim antara on-premises dan Azure dienkripsi dan aman dari akses yang tidak sah.

b. Azure Virtual Network (VNet):

1. Azure Virtual Network (VNet) menciptakan isolasi jaringan yang aman di cloud untuk semua resource Azure yang digunakan oleh perusahaan. Ini memungkinkan resource Azure untuk berkomunikasi secara aman satu sama lain.
2. VNet dibagi menjadi beberapa subnet, misalnya, satu subnet untuk web servers (Frontend Layer) dan satu subnet untuk application servers (Backend Layer).

c. Network Security Groups (NSGs):

1. SGs mengontrol lalu lintas jaringan masuk dan keluar ke resource Azure. Ini memungkinkan perusahaan dapat untuk menentukan aturan keamanan yang membatasi akses hanya pada traffic yang diperlukan.
2. Setiap subnet (misalnya, web servers dan application servers) dilindungi oleh NSG yang mengatur aturan inbound dan outbound untuk traffic jaringan. NSG memastikan bahwa hanya traffic yang diizinkan dapat mencapai resource tersebut.

5. Keamanan Komputasi atau **Layer 5**: Melibatkan perlindungan perangkat pengguna akhir dari ancaman seperti malware dan serangan siber. Prosedur yang digunakan membantu menjaga integritas dan keamanan perangkat yang terhubung ke jaringan.

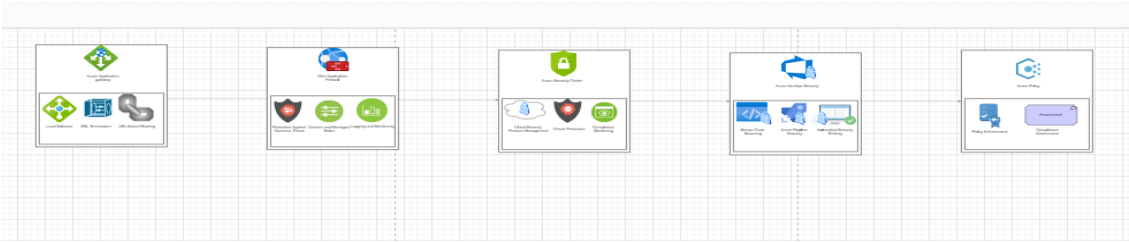
Gambar 5. Keamanan Komputasi

a. **Azure Security Center:**
   1. Monitor and Assess Security Posture: Azure Security Center memonitor semua resource Azure, termasuk virtual machines dan database. Ini melibatkan analisis keamanan secara terus-menerus untuk mengidentifikasi potensi risiko dan kelemahan keamanan.
   2. Security Center mengumpulkan data dari resource ini dan menggunakan algoritma analitik serta kecerdasan ancaman untuk menilai posture keamanan mereka.

b. **Recommendations and Alerts:**
   1. Berdasarkan penilaian yang dilakukan, Azure Security Center memberikan rekomendasi keamanan untuk memperbaiki kelemahan yang teridentifikasi. Rekomendasi ini bisa berupa konfigurasi ulang keamanan, penambalan kerentanan, atau tindakan lain untuk meningkatkan keamanan.
   2. Security Center juga memberikan peringatan (alerts) jika terdeteksi ancaman atau anomali yang membutuhkan perhatian segera.

c. **Implement Recommendations:**
   1. Tim keamanan perusahaan atau administrator sistem dapat mengambil tindakan berdasarkan rekomendasi dan peringatan yang diberikan oleh Azure Security Center. Ini dapat melibatkan penyesuaian konfigurasi, penambahan kebijakan keamanan, atau perbaikan kerentanan di virtual machines dan database.

6. Keamanan Aplikasi atau **Layer 6**: Melindungi aplikasi dari ancaman baik dari dalam maupun luar organisasi menggunakan berbagai alat dan teknik.



Gambar 6. Keamanan Aplikasi

Diagram ini mewakili arsitektur keamanan berlapis lainnya menggunakan berbagai layanan Azure, yang dirancang untuk meningkatkan keamanan dan kepatuhan lingkungan cloud. Berikut penjelasan rinci dari masing-masing komponen:

a. **Azure Application Gateway:**
   1. **Load Balancer**: Mendistribusikan lalu lintas masuk di beberapa server untuk memastikan ketersediaan dan keandalan yang tinggi.
   2. **Penghentian SSL**: Membongkar proses dekripsi SSL ke gateway, mengurangi beban pada server backend.
   3. **Web Application Firewall (WAF):** Melindungi aplikasi web dari ancaman dan kerentanan umum, seperti injeksi SQL dan skrip lintas situs (XSS).

b. **Jaringan Virtual Azure:**
   1. **Firewall**: Memberikan perlindungan tingkat jaringan dengan mengontrol lalu lintas masuk dan keluar.
   2. **Rute Kustom**: Menentukan aturan perutean tertentu untuk mengelola aliran lalu lintas dalam jaringan virtual.
   3. **ExpressRoute**: Membuat koneksi privat khusus antara jaringan lokal dan Azure, melewati internet publik.

c. Pusat Keamanan Azure:

1. **Manajemen Postur Keamanan Cloud**: Menilai postur keamanan sumber daya cloud dan memberikan rekomendasi untuk meningkatkan keamanan.
2. **Perlindungan Ancaman**: Menawarkan kemampuan deteksi dan perlindungan ancaman tingkat lanjut untuk melindungi dari ancaman dunia maya.
3. **Pemantauan Kepatuhan**: Melacak kepatuhan terhadap standar industri dan persyaratan peraturan, membantu memastikan kepatuhan.

d. Keamanan Azure DevOps:

1. **Pengembangan Kode Aman**: Menerapkan praktik terbaik keamanan di seluruh siklus hidup pengembangan perangkat lunak.
2. **Integrasi Azure Key Vault**: Menyimpan dan mengelola informasi sensitif seperti kunci dan rahasia API dengan aman.
3. **Infrastruktur sebagai Keamanan Kode**: Memastikan bahwa infrastruktur disebarkan dengan aman menggunakan otomatisasi berbasis kode dan praktik terbaik.

e. Kebijakan Azure:

1. **Penegakan Kebijakan**: Mengotomatiskan penerapan dan penerapan kebijakan organisasi di seluruh sumber daya Azure.
2. **Penilaian Kepatuhan**: Menyediakan alat untuk menilai dan melaporkan status kepatuhan, menyoroti area yang memerlukan perhatian atau perbaikan.

7. Keamanan Data atau **Layer 7**: Melibatkan perlindungan data yang disimpan dan yang sedang ditransmisikan melalui enkripsi dan kontrol akses untuk mencegah kebocoran data dan akses tidak sah. Implementasi kebijakan di lapisan ini memastikan perlindungan yang ketat terhadap data sensitif.

Gambar 7. Keamanan Data

Diagram ini mengilustrasikan arsitektur keamanan berlapis untuk lingkungan cloud, dengan fokus pada berbagai layanan Azure untuk perlindungan data dan manajemen ancaman. Berikut rincian komponennya:

a. Azure Data Lake Storage:

1. **Enkripsi Data**: Memastikan data dienkripsi saat tidak aktif dan dalam perjalanan, melindungi informasi sensitif dari akses yang tidak sah(Sukarna et al., 2023).
2. **Kontrol Akses**: Mengelola izin dan akses ke data, memastikan hanya pengguna yang berwenang yang dapat mengakses kumpulan data tertentu.

b. Azure SQL Database:

1. **Deteksi Ancaman**: Memantau dan mendeteksi aktivitas yang tidak biasa atau potensi ancaman dalam database(Nugraha & Chandra, 2023).
2. **Enkripsi Data**: Mengenkripsi data yang disimpan dalam database SQL untuk melindungi dari pelanggaran data.
3. **Keamanan Data Tingkat Lanjut**: Menyediakan lapisan keamanan tambahan, termasuk penilaian kerentanan dan perlindungan ancaman tingkat lanjut.

c. Azure Key Vault:

1. **Manajemen Rahasia**: Menyimpan dan mengelola informasi sensitif dengan aman seperti kunci API, kata sandi, dan rahasia lainnya.
2. **Manajemen Kunci**: Mengelola kunci kriptografi yang digunakan untuk enkripsi data.
3. **Manajemen Sertifikat**: Menangani sertifikat SSL/TLS untuk komunikasi yang aman.

d. Pusat Keamanan Azure:

1. **Klasifikasi Data**: Mengidentifikasi dan mengklasifikasikan data berdasarkan sensitivitas dan kepentingan.
2. **Perlindungan Ancaman**: Memberikan deteksi ancaman dan rekomendasi keamanan secara real-time untuk melindungi lingkungan.
3. **Pemantauan Kepatuhan**: Memantau dan melaporkan kepatuhan terhadap standar dan peraturan industri.

e. Kebijakan Azure:

1. **Penegakan Kebijakan**: Mengotomatiskan penegakan kebijakan keamanan untuk memastikan sumber daya mematuhi persyaratan organisasi dan peraturan.
2. **Penilaian Kepatuhan**: Menilai status kepatuhan lingkungan dan mengidentifikasi area yang perlu ditingkatkan

KESIMPULAN

Implementasi strategi keamanan siber yang komprehensif menggunakan layanan Microsoft Azure telah terbukti menjadi solusi efektif untuk mengatasi tantangan yang dihadapi oleh platform perusahaan start-up ini. Dengan menerapkan pendekatan "Seven Layer Defense in Depth", strategi ini meningkatkan keamanan platform di berbagai lapisan, mulai dari keamanan fisik hingga keamanan aplikasi. Pendekatan ini memastikan bahwa data pengguna dilindungi melalui manajemen identitas dan akses yang kuat, enkripsi data, dan mekanisme deteksi dan respons ancaman yang proaktif. Selain itu, strategi ini memfasilitasi kepatuhan terhadap regulasi perlindungan data yang ketat, seperti GDPR, sehingga meningkatkan kepercayaan pengguna terhadap platform. Penelitian ini menekankan pentingnya memanfaatkan layanan cloud canggih untuk membangun lingkungan pelatihan virtual yang skalabel, aman, dan patuh.

SARAN

1. **Pemantauan dan Peningkatan Berkelanjutan:** Secara berkala memperbarui dan meningkatkan protokol keamanan untuk mengikuti perkembangan ancaman siber. Implementasikan pemantauan berkelanjutan untuk mengidentifikasi dan mengatasi potensi kerentanan dengan cepat.
2. **Edukasi Pengguna:** Memberikan edukasi kepada pengguna tentang praktik terbaik untuk menjaga keamanan akun mereka, termasuk penggunaan kata sandi yang kuat dan mengaktifkan otentikasi multi-faktor.
3. **Audit Keamanan Berkala:** Melakukan audit keamanan secara berkala untuk memastikan kepatuhan terhadap persyaratan regulasi dan mengidentifikasi area yang perlu ditingkatkan dalam strategi keamanan siber.
4. **Kolaborasi dengan Ahli Keamanan:** Berkolaborasi dengan ahli keamanan siber dan memanfaatkan wawasan mereka untuk memperkuat posisi keamanan platform.
5. **Perencanaan Skalabilitas:** Merencanakan skalabilitas untuk memastikan bahwa platform dapat menangani peningkatan jumlah pengguna tanpa mengorbankan keamanan atau kinerja.

DAFTAR PUSTAKA

Antoni, M. S., & Suharjana, S. (2019). Aplikasi kebugaran dan kesehatan berbasis android: Bagaimana persepsi dan minat masyarakat? *Jurnal Keolahragaan*, *7*(1), 34–42. https://doi.org/10.21831/jk.v7i1.21571

Anugerah, M., Anugerah Nurrobi, M., & Syamsuar, D. (2022). Membuat Web Dengan VM Linux Menggunakan Microsoft Azure. Syntax Literate. *Jurnal Ilmiah Indonesia*, *7*(7). 10231- 10239

Mulyapati, R., & Agasia, W. (n.d.). Perancangan Startup Bayarape.Com Payment Point Dengan

Metode Pembayaran COD. *Jurnal ENTER. Volume 2*. 292-305.

Nazario Istalaksana, A., Muhammad, E., Jonemaro, A., & Akbar, M. A. (2022). Pengembangan Sistem Aplikasi Latihan Kebugaran pada Pemula berbasis Android. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer. 6*(1). 192-196. http://j-ptiik.ub.ac.id

Ningsih, A. A., Rambe, R. S., Munthe, Y. N., Sialalahi, P. R., William, J., Ps, I. V, Estate, M., Percut, K., Tuan, S., & Serdang, K. D. (2023). Pendekatan Lean Startup Pada Desain Produk Dan Teknik Minimum Viable Product Dalam Menyikapi Skeptisisme Pada Iklim Bisnis. *Jurnal Publikasi Sistem Informasi dan Manajemen Bisnis (JUPSIM)*. *2*(1). 183-198.

Nugraha, S., & Chandra, D. W. (2023). Peningkatan Keamanan Database Pada Layanan Azure Melalui Metode Multi-Tenant Dengan Pendekatan Separate Database. *Jurnal Pendidikan Dan Teknologi Indonesia*, *3*(6), 233–240. https://doi.org/10.52436/1.jpti.293

Purnaresa Yuliartanto dan Benfano Soewito. (2024). Pengembangan Aplikasi Aman Di Cloud Untuk Lean Startup. *INNOVATIVE: Journal Of Social Science Research.4*(2). 7891-7906

Sukarna, R. H., Januriana, A. M., . H., & Hilman, M. (2023). Implementasi Algoritma Enkripsi Pada Sistem Informasi Manajemen Helpdesk Berbasis Desktop. *Jurnal Informatika Dan Riset*, *1*(2), 31–39. https://doi.org/10.36308/iris.v1i2.535

Sulaksono, D. H., & Giovanni, A. R. (2020). *Implementasi Load Balancing Menggunakan Microsoft Azure*. *1*(2), 61–67.

Susanto, D., Ferdiana, R., & Sulistyo, S. (2022). Implementasi Laboratorium Komputer Virtual Berbasis Cloud-Kelas Pemrograman Berorientasi Obyek. In *Jurnal Nasional Teknik Elektro dan Teknologi Informasi*. *11*(1).ID-1-ID-7.

Chawro, S. (2022). *Microsoft Azure's defense in depth approach to cloud vulnerabilities.* Diakses tanggal 12 Desember 2024 dari https://azure.microsoft.com/en-us/blog/microsoft-azures-defense-in-depth-approach-to-cloud-vulnerabilities/