BAB I
PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi informasi dan percepatan transformasi digital mendorong organisasi untuk bergantung secara intensif pada layanan berbasis jaringan dan sistem informasi terintegrasi. PT Supra Primatama Nusantara (Biznet Networks) berperan sebagai penyelenggara infrastruktur digital terintegrasi yang menyediakan layanan internet berkecepatan tinggi, jaringan kabel bawah laut, data center, komputasi awan (cloud computing), dan IPTV guna mengurangi kesenjangan digital serta mendukung transformasi digital di berbagai sektor industri [3]. Di sisi lain, Biznet Data Center mengoperasikan fasilitas data center berskala besar di berbagai wilayah strategis yang dirancang dengan tingkat ketersediaan tinggi untuk menopang kebutuhan infrastruktur teknologi informasi perusahaan [4]. Skala dan kompleksitas infrastruktur tersebut menempatkan Biznet sebagai salah satu tulang punggung ekosistem ekonomi digital nasional sekaligus meningkatkan kebutuhan akan pengelolaan identitas dan akses yang aman, efisien, dan terukur pada berbagai sistem internal.

Pada tataran operasional, perusahaan seperti Biznet umumnya mengoperasikan beragam sistem kritikal, antara lain sistem manajemen sumber daya manusia, sistem keuangan, sistem monitoring jaringan, platform layanan pelanggan, sistem tiket gangguan, dan layanan surat elektronik korporat. Apabila setiap sistem mengelola akun dan kredensial pengguna secara terpisah, kondisi tersebut dapat menimbulkan duplikasi akun, ketidakkonsistenan hak akses, meningkatnya beban administrasi, serta kesulitan dalam melakukan penelusuran (audit trail) ketika terjadi insiden keamanan. Studi mutakhir mengenai identity and access management (IAM) menunjukkan bahwa model pengelolaan identitas yang terfragmentasi meningkatkan permukaan serangan, menyulitkan penerapan prinsip least privilege, dan menghambat kemampuan organisasi dalam merespons insiden keamanan secara cepat dan terukur [1]. Implementasi IAM terpusat direkomendasikan untuk menyatukan kebijakan akses, menyederhanakan siklus

hidup akun pengguna, serta menyediakan kontrol dan visibilitas yang lebih baik atas aktivitas autentikasi dan otorisasi di seluruh ekosistem aplikasi [1].

Salah satu fondasi teknis yang banyak digunakan dalam IAM terpusat adalah Lightweight Directory Access Protocol (LDAP). LDAP berfungsi sebagai layanan direktori yang menyimpan data identitas pengguna, struktur organisasi, grup, dan kebijakan akses dalam satu repositori terpusat yang dapat dimanfaatkan berbagai layanan dan aplikasi. Praktik industri dan kajian teknis menunjukkan bahwa direktori LDAP atau Active Directory secara luas dimanfaatkan sebagai sumber kebenaran tunggal untuk autentikasi dan otorisasi pada lingkungan enterprise, serta dapat diintegrasikan dengan protokol dan kerangka kerja lain, seperti Remote Authentication Dial-In User Service (RADIUS), Kerberos, OAuth 2.0, dan Security Assertion Markup Language (SAML), untuk mendukung skenario autentikasi terpusat dan Single Sign-On (SSO) [8]. Pendekatan ini secara signifikan mengurangi redundansi data identitas dan mempermudah pengelolaan hak akses ketika terjadi perubahan status karyawan maupun pemutakhiran kebijakan keamanan [1], [8].

Dari sisi pengalaman pengguna dan efisiensi operasional, mekanisme SSO menjadi komponen penting dalam arsitektur autentikasi modern. SSO memungkinkan pengguna melakukan autentikasi satu kali untuk kemudian mengakses berbagai aplikasi dan layanan internal tanpa harus berulang kali memasukkan kredensial yang sama. Namun, studi empiris terhadap implementasi SSO berbasis OpenID Connect dan OAuth 2.0 menunjukkan bahwa, di samping peningkatan kenyamanan, terdapat implikasi serius terhadap privasi dan keamanan, antara lain potensi pelacakan perilaku pengguna oleh identity provider, serangan session hijacking, serta kerentanan konfigurasi yang dapat dimanfaatkan untuk eskalasi hak akses [2], [5]. Hal ini menegaskan bahwa integrasi SSO dengan LDAP di lingkungan perusahaan harus dirancang dengan kontrol keamanan komprehensif, termasuk penguatan pada sisi identity provider, penggunaan mekanisme pertahanan berlapis, dan pemantauan berkelanjutan terhadap pola akses.

Perkembangan spektrum ancaman siber dan perubahan pola kerja modern, seperti remote working dan pemanfaatan multi-cloud, juga mendorong pergeseran paradigma keamanan dari pendekatan perimeter tradisional menuju Zero Trust

Architecture (ZTA). NIST melalui Special Publication 800-207 mendefinisikan Zero Trust sebagai seperangkat paradigma keamanan yang menghilangkan asumsi kepercayaan bawaan terhadap entitas di dalam maupun di luar jaringan, dengan penekanan pada verifikasi eksplisit, pemantauan berkelanjutan, dan pengambilan keputusan akses berbasis konteks [6]. Dalam kerangka ZTA, identitas pengguna dan perangkat ditempatkan sebagai perimeter utama, sementara kontrol akses ditegakkan secara granular dengan prinsip never trust, always verify [6]. Pada lingkungan multi-cloud, pendekatan Zero Trust Identity and Access Management dipandang penting untuk menyatukan kebijakan identitas lintas berbagai platform cloud sehingga organisasi dapat mempertahankan konsistensi kontrol akses dan keselarasan dengan profil risiko yang dinamis [7]. Demikian pula, model layanan Software as a Service (SaaS) memperkuat urgensi penerapan kontrol identitas yang konsisten di seluruh layanan pihak ketiga.

Dengan mempertimbangkan kompleksitas infrastruktur dan ragam sistem internal yang dioperasikan, Biznet Networks memerlukan arsitektur autentikasi dan otorisasi yang terpusat, aman, terukur, dan mudah diaudit [3], [4]. Tanpa integrasi yang kuat antara direktori terpusat berbasis LDAP, mekanisme SSO, dan prinsip Zero Trust, pengelolaan identitas karyawan dan akun layanan internal berpotensi tetap terfragmentasi, tidak efisien, serta lebih rentan terhadap penyalahgunaan kredensial, akses tidak sah, dan kesulitan penelusuran insiden. Kondisi tersebut membentuk urgensi perancangan dan implementasi sistem autentikasi terpusat berbasis LDAP yang terintegrasi dengan SSO dan selaras dengan prinsip Zero Trust di lingkungan Biznet Networks sebagai upaya peningkatan keamanan, efisiensi operasional, dan tata kelola akses pada infrastruktur digital yang dikelola perusahaan.

1.2. Rumusan Masalah

Berdasarkan latar belakang tersebut, dapat dirumuskan bahwa bagaimana penerapan sistem autentikasi terpusat berbasis LDAP dapat meningkatkan efisiensi manajemen data karyawan dan pengelolaan hak akses, sekaligus menjamin keamanan proses autentikasi serta konsistensi data identitas di seluruh layanan dan aplikasi internal perusahaan.

1.3. Tujuan Kegiatan

Kegiatan PKL ini bertujuan untuk mengetahui dan memahami penerapan pengelolaan data karyawan dan aset berbasis direktori terpusat serta mekanisme pengaturan hak akses karyawan sesuai peran dan tanggung jawabnya di PT Supra Primatama Nusantara (Biznet Networks).

1.4. Manfaat Kegiatan

1.4.1. Manfaat Bagi Perusahaan

1. Mendapatkan tenaga kerja potensial yang dapat membantu menyelesaikan tugas operasional dan meningkatkan produktivitas.
2. Membangun hubungan yang baik dengan institusi pendidikan sebagai bentuk kolaborasi dan kontribusi dalam pengembangan sumber daya manusia berkualitas.

1.4.2. Manfaat bagi UPN "Veteran" Jawa Timur

1. Memperluas koneksi dan jaringan kerja sama antara UPN "Veteran" Jawa Timur dan mitra perusahaan.
2. Membawa reputasi universitas ke jenjang yang lebih tinggi dan dikenal secara luas oleh industri.
3. Membuka peluang kolaborasi dengan universitas atau lembaga lain yang bekerja sama dengan mitra perusahaan.

1.4.3. Manfaat bagi Mahasiswa

1. Menerapkan ilmu yang diperoleh dalam dunia nyata, khususnya terkait data dan keamanan Sistem Informasi.
2. Meningkatkan kemampuan komunikasi dan menyiapkan mahasiswa untuk memasuki dunia kerja dengan pengalaman praktis.
3. Mengembangkan keterampilan pemecahan masalah serta mendapatkan pengalaman langsung dalam menangani isu keamanan sistem informasi