

IMPLEMENTASI KEBIJAKAN GRUP POLICY UNTUK MITIGASI RISIKO KEAMANAN PADA SERVER DI PT XYZ

¹Alissa Nabillah*, ²Muhammad Rifqi, ³Siti Maesaroh
^{1,2,3}Computer Science Faculty, Mercu Buana University, Indonesia

E-mail: ¹41520010168@student.mercubuana.ac.id, ²m.rifqi@mercubuana.ac.id,
³Siti.maesaroh@mercubuana.ac.id.

Abstract

PT XYZ needs to maintain a balance between operational efficiency and system security through the implementation of appropriate controls, especially in USB usage and server time management. Active Directory, a Windows Server feature, enables more efficient organizational security management by providing a basic database for user and device information across the network. The Group Policy feature in Active Directory also supports more effective management of computers and users on the network, helping companies maintain the integrity, authenticity, and availability of network resources. This study aims to test the application of these technologies to improve security and data management at PT XYZ.

Keywords : *Tuition Payment Process, Midtrans Payment Gateway, PIECES*

PENDAHULUAN

PT XYZ merupakan salah satu perusahaan televisi swasta di Indonesia. Perusahaan ini bergerak di bidang penyiaran dan hiburan. Mereka memiliki berbagai jenis program untuk menjangkau beragam minat pemirsa, mulai dari anak-anak hingga dewasa. Perusahaan ini memiliki infrastruktur teknologi yang sangat kompleks untuk mendukung semua program yang dilaksanakan oleh PT XYZ. Salah satu infrastruktur yang akan menjadi objek penelitian adalah server. Sejumlah pengguna, sumber daya, dan data akan dipusatkan pada satu server, yaitu Windows Server. Windows Server dapat digunakan sebagai sistem operasi yang dapat mengatur informasi data penting yang terdapat di PT XYZ..

Sistem komputer dan keamanan jaringan merupakan aspek krusial di era yang sedang berkembang pesatnya ancaman siber, era yang perkembangan ancaman sibernya semakin cepat. Salah satu aspek yang menjadi perhatian keamanan adalah penggunaan perangkat USB seperti flashdisk yang berpotensi terjadinya penyebaran data-data sensitif. Manajemen data juga memegang peranan penting untuk melindungi data-data rahasia suatu perusahaan dari ancaman virus yang mengakibatkan terjadinya korupsi data. Selain itu, manajemen data juga dapat melindungi data dari pihak luar yang ingin mencuri data-data penting suatu perusahaan [1]. Oleh karena itu, pembatasan penggunaan USB menjadi penting untuk mencegah potensi ancaman tersebut. Selain itu, sinkronisasi waktu melalui NTP Server juga memiliki peranan yang sangat penting dalam menjaga keakuratan log dan keamanan transaksi pada jaringan. Ketidakesesuaian waktu yang tepat dapat mengakibatkan terjadinya kerentanan keamanan yang cukup besar. Active Directory merupakan salah satu tools yang terdapat pada Windows Server, fitur ini cocok digunakan untuk mengelola keamanan suatu organisasi. Selain itu Active Directory dapat digunakan sebagai pusat database yang menyimpan informasi penting user dan endpoint yang digunakan oleh karyawan PT XYZ sehingga dapat memudahkan administrator dalam mengelolanya. Sehingga berperan dalam menjaga integritas, keaslian dan ketersediaan sumber daya jaringan. Dengan fitur yang dimiliki Active Directory, yaitu Group Policy yang dapat membantu perusahaan mengelola komputer dan pengguna pada jaringan dengan lebih efisien.

IMPLEMENTASI KEBIJAKAN GRUP POLICY UNTUK MITIGASI RISIKO KEAMANAN PADA SERVER DI PT XYZ

METODE PENELITIAN

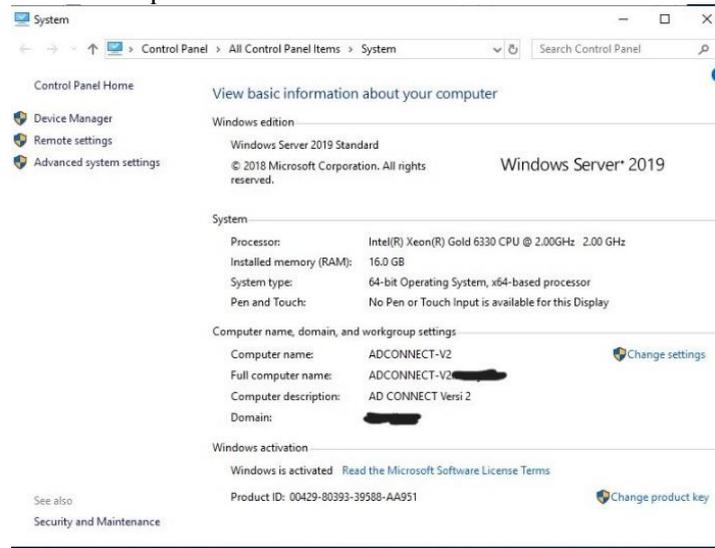
Salah satu langkah yang perlu dilakukan dalam penelitian adalah mengidentifikasi kekurangan, mencegah pengulangan metode yang sudah ada, dan mengetahui metode yang sudah pernah digunakan dan sedang digunakan oleh peneliti lain pada topik yang sama. Berikut ini adalah empat penelitian yang terkait dengan topik penelitian saat ini:

Pertama, Jurnal “Indigenous Secure NTP Server for Time Synchronization” tujuan utama penelitian ini adalah mengembangkan server Network Time Protocol (NTP) buatan dalam negeri yang aman untuk sinkronisasi waktu yang akurat pada jaringan sistem kontrol dan instrumentasi (C&I), khususnya untuk PLTN. Metode yang digunakan adalah merancang dan mengimplementasikan server NTP stratum-1 berbasis GPS menggunakan Field Programmable Gate Array (FPGA) tanpa sistem operasi. Hasilnya adalah pengembangan server NTP indigenous yang memiliki beberapa keunggulan dibandingkan produk komersial, termasuk desain OS-less yang lebih aman, dokumentasi yang luas yang memudahkan verifikasi dan validasi, dan fitur keamanan tambahan. Server ini mampu memproses 30.000 permintaan NTP per detik per port, dengan akurasi GPS maksimum ± 35 nanodetik [2]. Kedua, Jurnal “IMPLEMENTASI ACTIVE DIRECTORY DOMAIN SERVICES WINDOWS SERVER 2012 MENGGUNAKAN VMWARE HYPERVISOR VIRTUALISATION ESXi (STUDI KASUS PT-ETRANS)” Penelitian ini bertujuan untuk mengimplementasikan Active Directory Domain Services Windows Server 2012 menggunakan virtualisasi hypervisor VMware ESXi pada studi kasus di PT E-Trans. Sasarannya adalah untuk mengoptimalkan pengelolaan server, meningkatkan keamanan, dan mengefisienkan pengelolaan jaringan perusahaan. Metode yang digunakan meliputi pengumpulan data melalui observasi, wawancara, dan studi pustaka. Peneliti juga menggunakan pendekatan virtualisasi dengan VMware ESXi. Hasil penelitian menunjukkan bahwa implementasi Active Directory Domain Services pada Windows Server 2012 menggunakan virtualisasi VMware ESXi berhasil. Sistem ini memberikan solusi yang efisien dan terintegrasi untuk pengelolaan jaringan perusahaan, meningkatkan keamanan, dan memberikan fleksibilitas dalam pengaturan hak akses dan struktur jaringan. Secara keseluruhan, implementasi ini merupakan solusi untuk meningkatkan kualitas infrastruktur teknologi informasi di PT E-Trans [3]. Ketiga, Jurnal “Open Source Based Active Directory Implementation Using Linux and Samba 4” menguraikan tentang proses implementasi yang meliputi konfigurasi perangkat jaringan, manajemen user dan group, konfigurasi hardware, dan kebijakan keamanan dengan menggunakan metode Network Development Life Cycle (NDLC). Keunggulan jurnal ini adalah dengan menggunakan Active Directory Samba 4 dan Linux, data-data user dapat tersimpan dan diakses dengan baik sesuai dengan kebijakan yang telah ditetapkan. Hal ini membantu mencegah terjadinya pencurian data dan kerusakan data yang disebabkan oleh pihak-pihak yang tidak berwenang. Namun demikian, terdapat kelemahan jika hanya membahas implementasi Active Directory Samba 4 berbasis open source dengan menggunakan Linux. Pada jurnal-jurnal sebelumnya, implementasi Active Directory menggunakan sistem operasi Linux yaitu Samba 4, sedangkan pada penelitian ini menggunakan sistem operasi Windows Server dengan menetapkan beberapa kebijakan pada Group Policy Object [4]. Keempat, Jurnal “APLIKASI KONFIGURASI SERVER TERPUSAT BERBASIS WEB LINUX DI PT. XYZ” bertujuan untuk meningkatkan kontrol dan monitoring aktivitas administrator sistem pada server berbasis Linux yang digunakan di PT. XYZ. Penelitian ini menekankan pada pengembangan aplikasi berbasis web yang dapat mengelola server secara terpusat, terutama dalam hal instalasi, konfigurasi, dan kontrol perangkat lunak yang digunakan pada server. Metode yang digunakan dalam penelitian ini adalah metodologi Waterfall, yang memberikan pendekatan sekuensial dalam pengembangan perangkat lunak, mulai dari komunikasi, perencanaan, pemodelan, konstruksi, hingga deployment. Penelitian ini juga menggunakan protokol SNMP dan NTP untuk melakukan monitoring dan sinkronisasi server. Hasil penelitian ini menunjukkan bahwa aplikasi yang diusulkan dapat menggantikan penggunaan command line interface (CLI) dengan antarmuka berbasis tombol yang lebih user

friendly, sehingga dapat mengurangi risiko kesalahan akibat kesalahan pengetikan. Aplikasi ini juga memungkinkan IT Manager untuk melakukan monitoring aktivitas administrator sistem secara real-time, serta memberikan informasi terkait penggunaan CPU, RAM, dan hard disk pada server, yang dapat digunakan sebagai bahan pertimbangan untuk kebutuhan perangkat keras di masa mendatang [5].

1. Windows Server

Windows Server 2019 merupakan sistem operasi yang digunakan untuk membangun jaringan LAN (Local Area Network) yang berorientasi pada klien-server. Keunggulan Windows Server 2019 antara lain kemudahan konfigurasi yang disediakan oleh Server Manager, yang memungkinkan pengguna untuk dengan mudah mengatur, memasang, dan menghapus peran atau fitur pada Windows Server 2019.



Gambar 1. Windows Server

2. Direktori Aktif

Direktori Aktif berguna sebagai layanan atau basis data yang menyimpan data tercatat tentang pengguna, perangkat, aplikasi, grup, izin hibah, dan mengelola semua informasi ini dalam struktur hierarki. Fungsi utamanya adalah untuk melakukan autentikasi (AuthN) dan otorisasi (AuthZ) terhadap pengguna dan komputer. Dengan berkembangnya jaringan, Direktori Aktif membantu dalam mengorganisasikan sejumlah besar pengguna ke dalam beberapa grup dan subdivisi [6].



Gambar 2. Active Directory

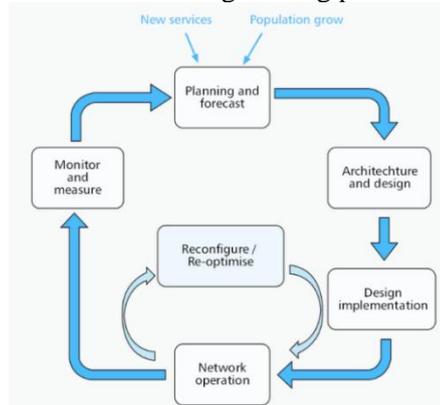
3. Encryption File System (EFS)

Kriptografi merupakan salah satu cabang ilmu matematika yang berfokus pada aspek keamanan informasi. Secara umum, kriptografi bertujuan untuk melindungi data dari akses yang tidak sah. Tujuan dari kriptografi adalah untuk melindungi pesan dari akses oleh pihak yang tidak berwenang dengan cara mengubah makna dari pesan tersebut [7]. Encryption File System (EFS) merupakan salah satu fitur keamanan pada platform Windows yang

IMPLEMENTASI KEBIJAKAN GRUP POLICY UNTUK MITIGASI RISIKO KEAMANAN PADA SERVER DI PT XYZ

digunakan untuk mengenkripsi file dan folder. Saat menggunakan EFS, hanya pemegang kunci enkripsi yang dapat mengetahui informasi tersebut. memiliki izin untuk membuka dan mengakses konten file atau folder terenkripsi. EFS menggunakan teknik enkripsi asimetris yang melibatkan sepasang kunci: kunci publik untuk enkripsi dan kunci pribadi untuk dekripsi.

4. Metode Network Life Cycle digunakan sebagai pedoman utama dalam proses pengembangan dan perancangan sistem jaringan komputer secara keseluruhan atau secara umum. Hal ini dikarenakan dalam menghadapi kebutuhan dan permasalahan sistem jaringan terdapat kebutuhan, permasalahan, dan solusi yang berbeda-beda. Oleh karena itu, diperlukan pendekatan metode Network Life Cycle yang beragam agar dapat memberikan solusi yang sesuai dengan karakteristik masing-masing permasalahan yang muncul [8].



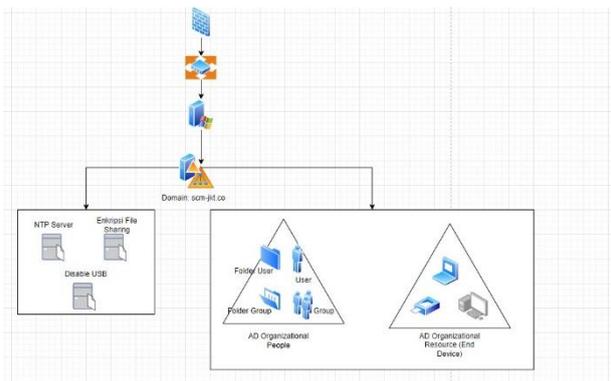
Gambar : 3. Network Life Cycle

Pada tahap ini direncanakan spesifikasi perangkat keras yang akan digunakan dalam penelitian ini. PT. XYZ menggunakan Windows Server 2019 sebagai host server. Client yang akan digunakan sebagai salah satu contoh uji coba penelitian ini adalah Windows 11.

Table 1. Hardware Specifications

<i>Hardware</i>	Specifications
<i>Server Host</i>	Processor Intel® Xeon® Gold 6330 CPU @ 2.00GHz.
<i>Client</i>	Memory (Random Access Memory) 16.00 GB Processor 11th Gen Intel(R) Core(TM) i5-1135G7 @ 2.40GHz 1.38 GHz Memory (Random Access Memory) 8.00 GB

Merancang arsitektur jaringan dan merancang konfigurasi Direktori Aktif, sinkronisasi waktu Server NTP, enkripsi data Server File, dan aturan Objek Kebijakan Grup untuk pembatasan penggunaan USB berdasarkan perencanaan pada tahap sebelumnya.



Gambar 4 : . Configuration Design

5. Pengumpulan Data

Metode yang digunakan untuk mengumpulkan data adalah sebagai berikut:

1) Studi Literatur

Data diperoleh dari literatur, jurnal, dan studi literatur yang terkait dengan implementasi kebijakan keamanan, Group Policy Active Directory, dan topik terkait lainnya. Data sekunder ini dapat mendukung pemahaman dan analisis dalam penelitian.

2) Observasi Observasi merupakan metode pengumpulan data dengan cara mengamati secara langsung objek penelitian [9]. Dalam penelitian ini, observasi akan mencakup data pengguna di divisi IT lantai 8 PT XYZ.

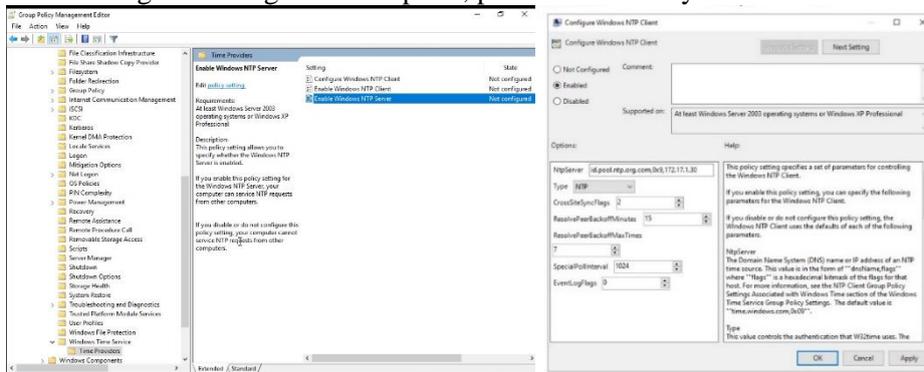
3) Wawancara

Wawancara merupakan metode pengumpulan data melalui sesi tanya jawab terstruktur yang dilakukan secara satu arah, berdasarkan tujuan penelitian [10]. Dalam penelitian ini, wawancara dilakukan untuk melengkapi data penelitian dengan cara mengajukan pertanyaan kepada para ahli di bidang administrator sistem.

HASIL DAN PEMBAHASAN

1. Sinkronkan Waktu Server dengan Klien

Siapkan sinkronisasi waktu setiap 24 jam secara otomatis menggunakan Penjadwal Tugas. Klik kanan pada kebijakan Sinkronisasi Waktu dan pilih edit, dan Editor Manajemen Kebijakan Grup akan muncul. Di bagian Konfigurasi Komputer, pilih Sistem > Layanan Waktu Windows.



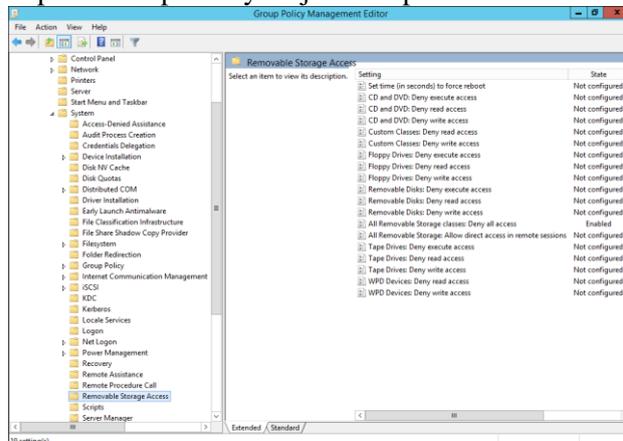
Gambar 4. Enable NTP Client Configuration

Pada Windows Time Service pilih folder Time Providers, lalu double klik Enable Windows NTP Server untuk mengaktifkan fitur NTP Server. Double klik pada opsi Configure Windows NTP Client, NtpServer diisi dengan IP Address Windows Server. Type diubah menjadi NTP. Sehingga semua client yang terhubung ke jaringan server diatur sesuai dengan waktu di server.

2. Pembatasan Akses Penggunaan USB (Disable USB)

IMPLEMENTASI KEBIJAKAN GRUP POLICY UNTUK MITIGASI RISIKO KEAMANAN PADA SERVER DI PT XYZ

Batasi penggunaan USB melalui Group Policy di sisi endpoint pengguna agar tidak terjadi penyebaran data penting. Atur Disable USB via Group Policy Object dengan masuk ke Group Policy Management dan klik kanan pada Group Policy Object lalu pilih new.

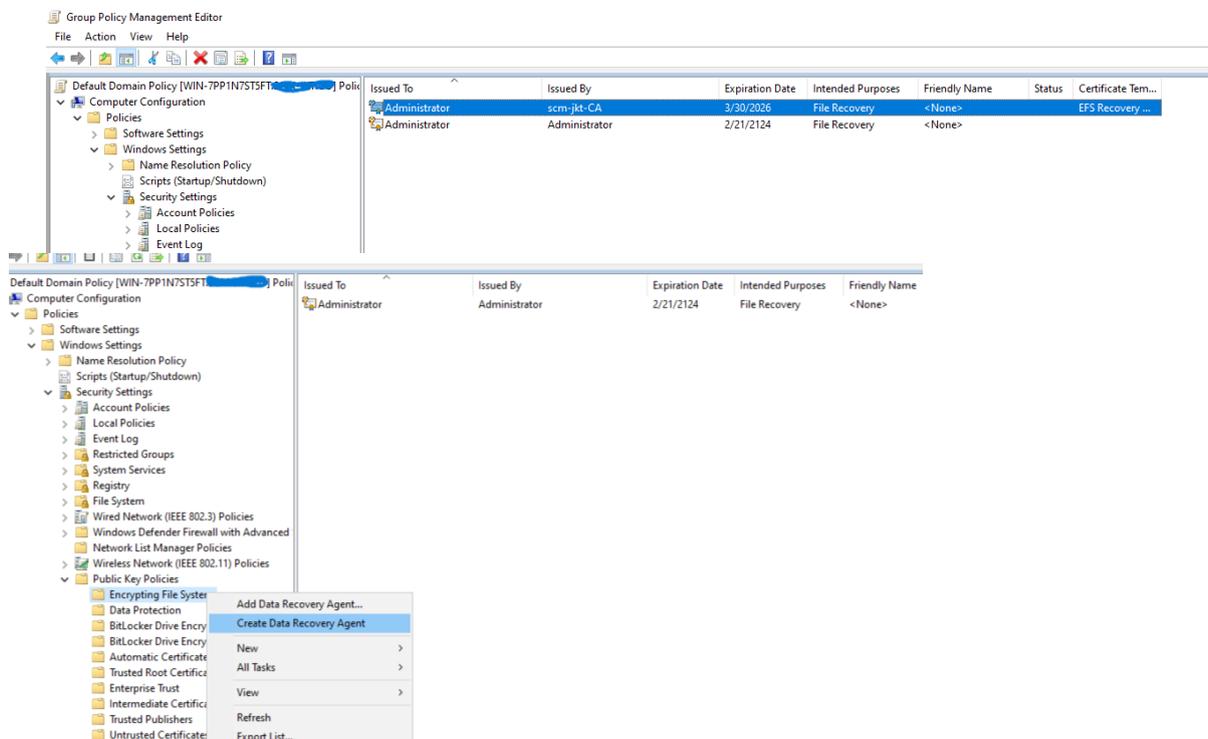


Gambar 6. Removable Disk

Klik kanan pada kebijakan Disable USB dan pilih edit, maka akan muncul Group Policy Management Editor. Pada bagian Computer Configuration pilih System > Removable Storage Access. Klik dua kali pada All Removable Storage classes: Deny all access untuk mengaktifkan fitur tersebut, sehingga semua Removable Storage seperti USB akan dinonaktifkan/tidak terbaca pada sistem.

3. Enkripsi File Server Dengan EFS

Keamanan informasi merupakan upaya untuk mencegah akses, penggunaan, pengungkapan, gangguan, modifikasi, atau penghancuran informasi secara ilegal atau tidak sah. Hal ini dilakukan agar informasi tetap aman, lengkap, dan dapat diakses oleh pihak yang berwenang setiap kali dibutuhkan [11].



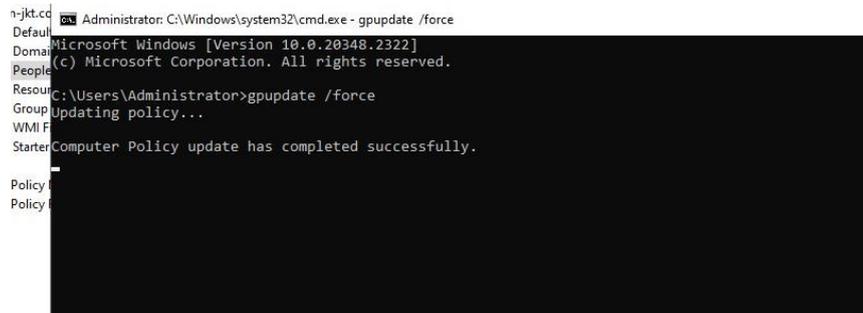
Gambar 5. Data Recovery Agent

Penambahan Data Recovery Agent (DRA) digunakan untuk memulihkan akses ke data yang

dienkripsi dengan Encrypting File System (EFS) jika pengguna kehilangan kunci enkripsinya.

4. Operasi Jaringan

Setelah diimplementasikan, semua konfigurasi kemudian akan dioperasikan dan digunakan oleh pengguna atau klien. Agar semua kebijakan dapat berjalan di endpoint, jalankan perintah gpupdate /force di Command Prompt. Lakukan di server dan juga klien endpoint. Sehingga semua kebijakan yang telah diterapkan berhasil digunakan.

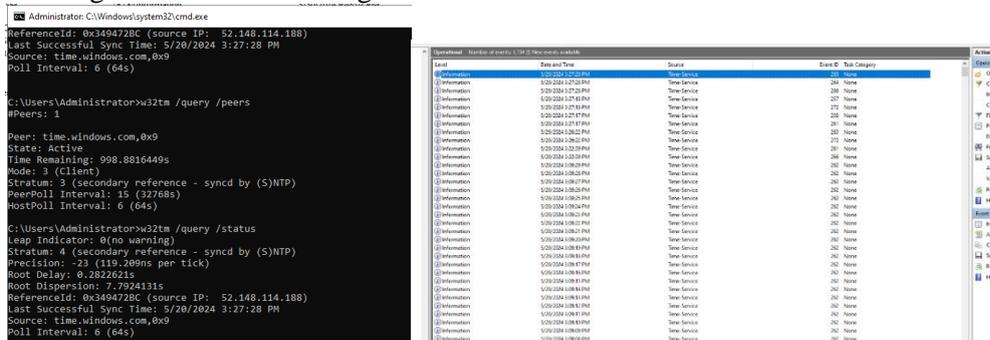


Gambar 6. Running All Policy

Setelah mengimplementasikan beberapa policy melalui group policy object, setelah itu pastikan apakah semua policy tersebut berhasil diimplementasikan melalui endpoint yang digunakan oleh PT XYZ

1 Pengujian Keberhasilan Sinkronisasi Waktu

Pengujian keberhasilan penggunaan Group Policy untuk keamanan Active Directory dilakukan dengan menggunakan satu Client atau endpoint yang terhubung dalam satu jaringan dengan server dan harus join pada domain yang sudah ada. Dengan menjalankan perintah w32tm /query /status yang berguna untuk mengecek apakah sistem sudah tersinkronisasi tepat waktu dengan sumber waktu eksternal, untuk menghindari masalah seperti security vulnerability atau inkonsistensi log. Log akan disimpan setiap kali server melakukan atau berhasil melakukan sinkronisasi waktu antara client dan server dengan melihat sesuai dengan nomor Event ID.

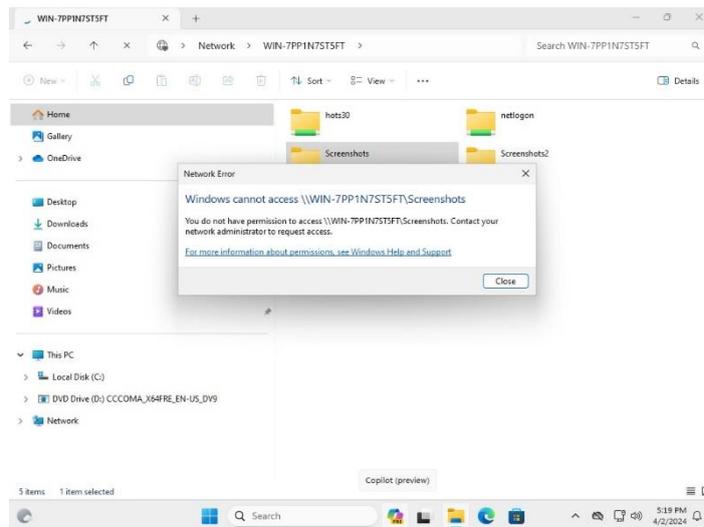


Gambar 7. Checking Synchronization Status

2. Pengujian Keberhasilan Enkripsi Data Menggunakan EFS

Penggunaan enkripsi data seperti Encrypting File System (EFS) dapat menjadi langkah penting, dengan menerapkan enkripsi pada file yang menyimpan informasi sensitif, administrator divisi IT PT XYZ dapat memastikan bahwa data hanya dapat diakses oleh pihak yang memiliki kunci enkripsi yang sesuai. Hal ini tidak hanya meningkatkan keamanan data internal, tetapi juga memberikan perlindungan ekstra saat berbagi file dengan pihak eksternal, seperti mitra produksi, distributor, atau penyedia layanan lainnya.

IMPLEMENTASI KEBIJAKAN GRUP POLICY UNTUK MITIGASI RISIKO KEAMANAN PADA SERVER DI PT XYZ

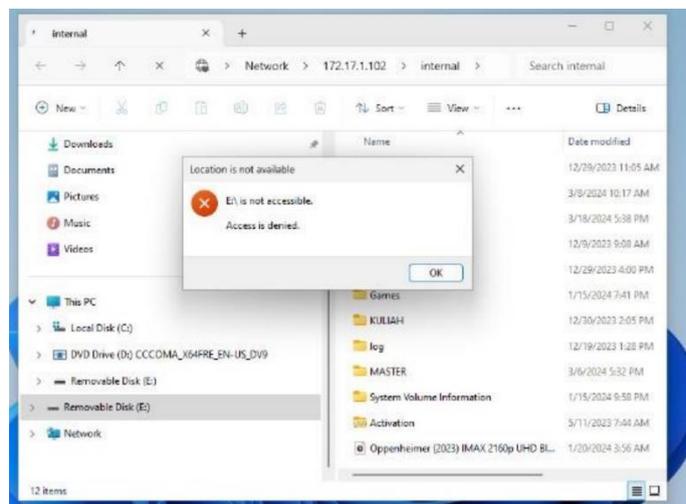


Gambar 8. Unauthorized Folder Access

Misalnya, seorang pengguna ingin mengakses data di server, tetapi data tersebut hanya dapat diakses oleh administrator. Dengan menggunakan enkripsi EFS, pengguna tidak dapat membuka folder/file tersebut. Dengan demikian, penggunaan enkripsi data menjadi bagian integral dari strategi keamanan informasi PT XYZ, yang membantu menjaga kerahasiaan, integritas, dan keandalan data mereka dalam industri yang kompetitif.

3 Pengujian Keberhasilan USB Disable

Setelah penerapan USB Disable, perusahaan telah mencegah insiden keamanan yang terkait dengan penggunaan perangkat penyimpanan USB yang tidak sah. Risiko kebocoran data dan infeksi malware berkurang, sehingga integritas dan keamanan data perusahaan tetap terjaga. Selain itu, kebijakan ini juga telah meningkatkan kesadaran karyawan akan pentingnya keamanan data dan praktik terbaik dalam menggunakan perangkat penyimpanan eksternal.



Gambar 9. Disable USB

Gambar 11 adalah contoh saat pengguna yang tidak memiliki akses mencoba menggunakan USB ke komputer klien. Ada perintah Akses ditolak.

KESIMPULAN

Penerapan beberapa kebijakan untuk menjaga keamanan server Active Directory di PT XYZ dapat dilakukan melalui fitur Group Policy Object (GPO). Penelitian ini menunjukkan bahwa dengan menerapkan konfigurasi NTP Server, enkripsi data File Server, dan pembatasan penggunaan USB, perusahaan dapat secara efektif meningkatkan keamanan dan mengatasi potensi ancaman. Sinkronisasi waktu menggunakan NTP Server memastikan bahwa seluruh jaringan memiliki waktu yang akurat dan konsisten, yang penting untuk menghindari kerentanan keamanan dan masalah dengan log. Enkripsi data File Server menggunakan Encrypting File System (EFS) menjaga kerahasiaan dan integritas data perusahaan dan memberikan perlindungan tambahan saat berbagi file dengan pihak eksternal. Pembatasan penggunaan USB melalui kebijakan penonaktifan USB mencegah insiden keamanan yang terkait dengan penggunaan perangkat penyimpanan USB yang tidak sah, mengurangi risiko kebocoran data dan infeksi malware. Penelitian ini menerapkan metode Network Life Cycle untuk memastikan bahwa implementasi dilakukan secara terstruktur dan sistematis, mulai dari perencanaan hingga pemantauan hasil konfigurasi. Dengan menerapkan solusi keamanan ini, PT XYZ dapat meningkatkan keamanan jaringan dan melindungi data perusahaan dari ancaman internal dan eksternal. Penelitian ini menekankan pentingnya penerapan kebijakan keamanan yang tepat dalam lingkungan bisnis modern untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi.

DAFTAR PUSTAKA

- H. U. A. E. M. Ibnu Fatihul Busyro, "IMPLEMENTASI FITUR FILE SERVER RESOURCE MANAGER PADA SISTEM OPERASI WINDOWS SERVER 2019 UNTUK MEMPERMUDAH MANAJEMEN DOKUMEN SERVER," *JURNAL ADMINISTRASI JARINGAN KOMPUTER*, 2023.
- M. A. A. Handri Kusuma, "IMPLEMENTASI ACTIVE DIRECTORY DOMAIN SERVICES WINDOWS SERVER 2012 MENGGUNAKAN VIRTUALISASI HYPERVISOR VMWARE ESXI (STUDY KASUS PT-ETRANS)," *Jurnal Penelitian Ilmu Komputer*, vol. Vol. 1, 2023.
- I. F. Agus Fatulloh, "Implementasi Active Directory Berbasis Open Source Menggunakan Linux dan Samba 4," *JURNAL BIT*, vol. Vol. 17, 2020.
- M. Andi Nugroho, "APPLICATION CONFIGURATION CENTRALIZED LINUX WEB-BASED SERVER AT PT. XYZ," *International Research Journal of Computer Science (IRJCS)*, vol. Volume 5, no. Issue 05, 2018.
- A. M. K. H. G. W. Nalini C Iyer, "Implementation of Active Directory for efficient management of networks," *Elsevier*, 2019.
- M. Rifqi, "COMBINING STEGANOGRAPHY AND CRYPTOGRAPH TECHNIQUES FOR DATA SECURITY (CASE STUDY IN PT XYZ)," *International Research Journal of Computer Science (IRJCS)*, vol. Volume 5, no. Issue 01, 2018.
- E. P. R. Rachmad Fachruddin, "Penerapan File Sharing Terpusat Menggunakan Samba Server Pada Kantor Kecamatan Ratu Samban," *Jurnal Media Infotama*, 2022.
- I. R. Zainuddin Khaizar, "ANALYSIS AND DESIGN PRESENCE ONLINE APPLICATION PT.TELKOM AKSES," *International Research Journal of Computer Science (IRJCS)*, vol. Volume 5, no. Issue 05, 2018.
- I. G. Z. M. N. S. S. I. O. M. Fahri H Damanik, "PEMANFAATAN ALGORITMA AES UNTUK KEAMANANN DATA KARYAWAN PT. TELKOM INDONESIA PEMATANGSIANTAR," *Jurnal Ilmiah Teknik dan Ilmu Komputer*, vol. I, 2022.
- A. M. S. M. D. A. R. a. U. W. V. Abhishek Borana, "Indigenous Secure NTP Server for Time Synchronization," *C&I Network*, 2023.