Jurnal Manajemen Informatika Jayakarta
Volume 4, Nomor 3, Juli 2024: halaman 258-265

P-ISSN: 2746-5985
e-ISSN: 2797-0930

DOI: https://doi.org/10.52362/jmijayakarta.v4i3.1531

PENGEMBANGAN KEAMANAN KOMPUTER DENGAN TEKNOLOGI THIN CLIENT DAN DOMAIN CONTROLLER DENGAN METODE NETWORK DEVELOPMENT LIFE CYCLE (NDLC)

[1]Yogi Kristiyanto*, [2] Sugiyono, [3]Caesar Angga Perdana, [4]Siti Sarah

[1,3]Sistem Informasi, Fakultas Sains dan Kesehatan, Universitas IPWIJA
[2]Teknik Informatika, Fakultas Komputer, Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika
[4]Informatika, Fakultas Sains dan Kesehatan, Universitas IPWIJA
[1,3,4]Jl. Letda Nasir No.7, Nagrak, Kec.Gn.Putri, Kabupaten Bogor, JawaBarat 16966, (021) 8233737
[2]Jln. Raden Inten II No.8A, Duren Sawit, Jakarta Timur –DKI Jakarta, Indonesia, 021-8661 4332

*e-mail: yogi.kristiyanto@gmail.com , inosoguy007@gmail.com, caesar.a.perdana@gmail.com, sitisarah@ipwija.ac.id

Abstrak

Dalam era digital yang semakin maju, keamanan komputer menjadi prioritas utama bagi banyak organisasi. Judul penelitian ini, "Pengembangan Keamanan Komputer dengan Teknologi Thin Client dan Domain Controller Dengan Metode Network Development Life Cycle (NDLC)", mencerminkan kebutuhan akan solusi keamanan yang lebih andal dan efisien. Penelitian ini bertujuan untuk mengembangkan model keamanan komputer yang menggabungkan teknologi thin client dan domain controller. Metode yang digunakan adalah Network Development Life Cycle (NDLC), yang mencakup analisis kebutuhan, perancangan, implementasi, pengujian, dan pemeliharaan. Hasil penelitian diharapkan dapat menunjukkan peningkatan dalam keamanan jaringan dan efisiensi pengelolaan sumber daya IT. Berdasarkan peenjelasan tahapan NDLC tersebut pada subjek penelitian dapat dibuatkan sebagai berikut, yaitu dimana beberapa terminal Thin Client yang terhubung ke sebuah server yang menjalankan sistem operasi Windows Server dan berfungsi sebagai Domain Controller dengan Active Directory. Untuk perangkat Thin Client yang digunakan adalah NComputing dimana pada server di sistem operasi Windows Server tersebut juga terpasang aplikasi controller vSpace LTS dari NComputing. Pengembangan Keamanan Komputer dengan Teknologi Thin Client dan Domain Controller Dengan Metode Network Development Life Cycle (NDLC) adalah langkah yang potensial dalam meningkatkan efisiensi operasional dan keamanan sistem jaringan. Dengan pendekatan yang tepat, organisasi dapat mengoptimalkan penggunaan teknologi ini untuk mencapai tujuan bisnis mereka dengan aman dan efisien.

Kata kunci: Keamanan Komputer, Thin Client, Domain Controller, NComputing, Network Development Life Cycle.

Abstract

In an increasingly advanced digital era, computer security has become a top priority for many organizations. The title of this research, "Development of Computer Security with Thin Client and Domain Controller Technology Using the Network Development Life Cycle (NDLC) Method", reflects the need for more reliable and efficient security solutions. This research aims to develop a computer security model that combines thin client and domain controller technology. The method used is the Network Development Life Cycle (NDLC), which includes requirements analysis, design, implementation, testing and maintenance. The research results are expected to show improvements in network security and IT resource management efficiency. Based on the explanation of the NDLC

This work is licensed under a Creative Commons Attribution 4.0 International License.
http://journal.stmikjayakarta.ac.id/index.php/JMIJayakarta

Jurnal Manajemen Informatika Jayakarta
Volume 4, Nomor 3, Juli 2024: halaman 258-265
P-ISSN: 2746-5985
e-ISSN: 2797-0930

DOI: https://doi.org/10.52362/jmijayakarta.v4i3.1531

stages, the research subject can be created as follows, namely where several Thin Client terminals are connected to a server that runs the Windows Server operating system and functions as a Domain Controller with Active Directory. The Thin Client device used is NComputing where the server on the Windows Server operating system also has the vSpace LTS controller application from NComputing installed. Developing Computer Security using Thin Client and Domain Controller Technology Using the Network Development Life Cycle (NDLC) Method is a potential step in increasing operational efficiency and security of network systems. With the right approach, organizations can optimize the use of this technology to achieve their business goals safely and efficiently..

Keywords:. *Computer Security, Thin Client, Domain Controller, NComputing, Network Development Life Cycle.*

1 Pendahuluan

Dalam era digital yang semakin maju, keamanan komputer menjadi prioritas utama bagi banyak organisasi. Judul penelitian ini, "Pengembangan Keamanan Komputer dengan Teknologi Thin Client dan Domain Controller Dengan Metode Network Development Life Cycle (NDLC)", mencerminkan kebutuhan akan solusi keamanan yang lebih andal dan efisien. Thin client adalah perangkat komputasi yang bergantung pada server untuk melakukan sebagian besar pemrosesan [12], sementara domain controller adalah server yang mengelola keamanan jaringan dan identitas pengguna. Kombinasi kedua teknologi ini berpotensi menciptakan lingkungan komputasi yang lebih aman dan terkendali. Berbagai studi telah mengkaji manfaat teknologi thin client dan domain controller dalam meningkatkan keamanan jaringan[8]. Penelitian ini bertujuan untuk mengembangkan model keamanan komputer yang menggabungkan teknologi thin client dan domain controller. Metode yang digunakan adalah Network Development Life Cycle (NDLC), yang mencakup analisis kebutuhan, perancangan, implementasi, pengujian, dan pemeliharaan [2][11]. Hasil penelitian diharapkan dapat menunjukkan peningkatan dalam keamanan jaringan dan efisiensi pengelolaan sumber daya IT. Penelitian ini mencakup pembahasan tentang konsep thin client dan domain controller, metodologi NDLC dan proses implementasi. Data dikumpulkan melalui literasi dan studi kasus pada beberapa perusahaan yang telah mengimplementasikan teknologi ini.

2 Tinjauan Literatur

Penelitian sebelumnya menemukan bahwa thin client [1] adalah perangkat perhitungan akhir dengan aplikasi komunikasi terinstal yang memberikan operator produksi kemungkinan untuk bekerja dalam mode terminal. Aplikasi dikontrol dengan sistem operasi lokal untuk memuat dan menyimpan ke dalam memori di perangkat solidnya. Thin client berisi konfigurasi minimum sumber daya perhitungan dan berinteraksi dengan server terminal jarak jauh dalam mode client dan server. Thin client ramah lingkungan karena mereka memiliki lebih sedikit perangkat keras sehingga menghasilkan lebih sedikit limbah elektronik di akhir siklus hidupnya [13]. Sementara itu, dikutip dari Microsoft [10] Domain Controller menyediakan penyimpanan fisik untuk database Active Directory Domain Services (AD DS), selain menyediakan layanan dan data yang memungkinkan perusahaan mengelola server, workstation, pengguna, dan aplikasi mereka secara efektif. Jika akses istimewa ke pengontrol domain diperoleh, pengguna jahat dapat mengubah, merusak, atau menghancurkan database AD DS dan, lebih jauh lagi, semua sistem dan akun yang dikelola oleh Direktori Aktif. Salah satu pemeriksaan yang dilakukan sebagai bagian dari Penilaian Keamanan Direktori Aktif adalah penggunaan dan konfigurasi browser web pada pengontrol domain. Tidak ada browser web yang boleh digunakan pada pengontrol domain. Analisis terhadap ribuan pengontrol domain mengungkapkan banyak kasus di mana pengguna yang memiliki hak istimewa menggunakan Internet Explorer untuk menjelajahi intranet atau Internet organisasi. Penelitian ini mencoba menggabungkan kedua teknologi tersebut untuk mengevaluasi potensi sinergi dalam pengelolaan keamanan komputer berdasarkan metode Network Development Life Cycle (NDLC).

This work is licensed under a Creative Commons Attribution 4.0 International License.
http://journal.stmikjayakarta.ac.id/index.php/JMIJayakarta

Jurnal Manajemen Informatika Jayakarta
Volume 4, Nomor 3, Juli 2024: halaman 258-265
P-ISSN: 2746-5985
e-ISSN: 2797-0930

DOI: https://doi.org/10.52362/jmijayakarta.v4i3.1531

3 Metode Penelitian

Proses penelitian mengikuti tahapan NDLC yang terdiri dari lima tahap utama [6]:

- **Analisis Kebutuhan:** Mengidentifikasi kebutuhan bisnis dan teknis untuk meningkatkan keamanan dan efisiensi jaringan komputer.
- **Perancangan:** Merancang arsitektur sistem yang menggabungkan teknologi thin client dan domain controller.
- **Implementasi:** Mengimplementasikan desain yang telah dibuat dalam lingkungan perusahaan.
- **Pengujian:** Melakukan pengujian untuk memastikan bahwa sistem berfungsi sesuai dengan spesifikasi dan kebutuhan keamanan.
- **Pemeliharaan:** Menyediakan dukungan berkelanjutan untuk memastikan sistem tetap aman dan efisien.

Subjek penelitian adalah perusahaan yang telah atau berencana untuk mengimplementasikan teknologi thin client dan domain controller. Objek penelitian meliputi sistem jaringan komputer dan kebijakan keamanan yang diterapkan di perusahaan tersebut.

4 Hasil dan Pembahasan

Proses penelitian mengikuti tahapan Network Development Life Cycle (NDLC) yang terdiri dari lima tahap utama: analisis kebutuhan, perancangan, implementasi, pengujian, dan pemeliharaan. Setiap tahap dijelaskan secara rinci sebagai berikut,

Analisis Kebutuhan

Tahap analisis kebutuhan melibatkan identifikasi kebutuhan bisnis dan teknis yang harus dipenuhi untuk meningkatkan keamanan dan efisiensi jaringan komputer. Langkah-langkah dalam tahap ini meliputi:

- **Identifikasi Ancaman dan Risiko Keamanan:** Menilai potensi ancaman dan risiko yang dihadapi oleh jaringan komputer, seperti serangan malware, ransomware, dan akses tidak sah.
- **Evaluasi Infrastruktur Jaringan:** Meninjau infrastruktur jaringan yang ada untuk mengidentifikasi kelemahan dan area yang perlu ditingkatkan.
- **Kebutuhan Pengguna:** Mengumpulkan informasi dari pengguna tentang masalah yang dihadapi dan fitur yang diinginkan untuk meningkatkan produktivitas dan keamanan.
- **Tujuan Keamanan:** Menentukan tujuan keamanan, seperti memastikan integritas data, menjaga kerahasiaan informasi, dan memastikan ketersediaan sistem.

Perancangan

Tahap perancangan melibatkan pembuatan blueprint atau desain arsitektur sistem yang menggabungkan teknologi thin client dan domain controller. Aspek-aspek yang diperhatikan dalam perancangan meliputi:

- **Arsitektur Thin Client:** Merancang arsitektur thin client yang akan digunakan oleh pengguna akhir. Thin client merupakan perangkat yang minimalis yang bergantung pada server pusat untuk komputasi utama, sehingga mengurangi risiko serangan pada perangkat end-user.
- **Konfigurasi Domain Controller:** Merancang domain controller yang mengelola otentikasi, kebijakan keamanan, dan kontrol akses. Domain controller memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses sumber daya jaringan.
- **Integrasi Keamanan:** Merancang mekanisme keamanan seperti firewall, enkripsi, dan sistem deteksi intrusi yang akan diintegrasikan dalam arsitektur jaringan.
- **Rencana Pemulihan Bencana:** Merancang rencana pemulihan bencana untuk memastikan bahwa sistem dapat dipulihkan dengan cepat dalam hal kegagalan atau serangan.

Implementasi

This work is licensed under a Creative Commons Attribution 4.0 International License.
http://journal.stmikjayakarta.ac.id/index.php/JMIJayakarta

Jurnal Manajemen Informatika Jayakarta
Volume 4, Nomor 3, Juli 2024: halaman 258-265
P-ISSN: 2746-5985
e-ISSN: 2797-0930
DOI: https://doi.org/10.52362/jmijayakarta.v4i3.1531

Tahap implementasi melibatkan penerapan desain yang telah dibuat dalam lingkungan perusahaan. Langkah-langkah dalam tahap ini meliputi:

- **Instalasi Thin Client:** Menginstal dan mengonfigurasi perangkat thin client pada workstation pengguna.
- **Deploy Domain Controller:** Menginstal dan mengonfigurasi server domain controller untuk mengelola otentikasi dan kontrol akses.
- **Penerapan Kebijakan Keamanan:** Menerapkan kebijakan keamanan yang dirancang pada domain controller, seperti kebijakan password, akses remote, dan enkripsi data.
- **Pelatihan Pengguna:** Memberikan pelatihan kepada pengguna tentang penggunaan thin client dan pentingnya praktik keamanan yang baik.

Pengujian

Tahap pengujian melibatkan verifikasi dan validasi sistem untuk memastikan bahwa sistem berfungsi sesuai dengan spesifikasi dan memenuhi kebutuhan keamanan. Aktivitas pengujian meliputi:

- **Uji Fungsional:** Menguji fungsionalitas thin client dan domain controller untuk memastikan semua fitur bekerja sesuai yang diharapkan.
- **Uji Keamanan:** Melakukan uji penetrasi dan uji kerentanan untuk mengidentifikasi potensi celah keamanan.
- **Uji Kinerja:** Mengukur kinerja sistem untuk memastikan bahwa sistem dapat menangani beban kerja yang diharapkan tanpa degradasi kinerja.
- **Uji User Acceptance:** Melibatkan pengguna dalam pengujian untuk memastikan bahwa sistem memenuhi kebutuhan dan ekspektasi mereka.

Pemeliharaan

Tahap pemeliharaan melibatkan penyediaan dukungan berkelanjutan untuk memastikan bahwa sistem tetap aman dan efisien. Aktivitas pemeliharaan meliputi:

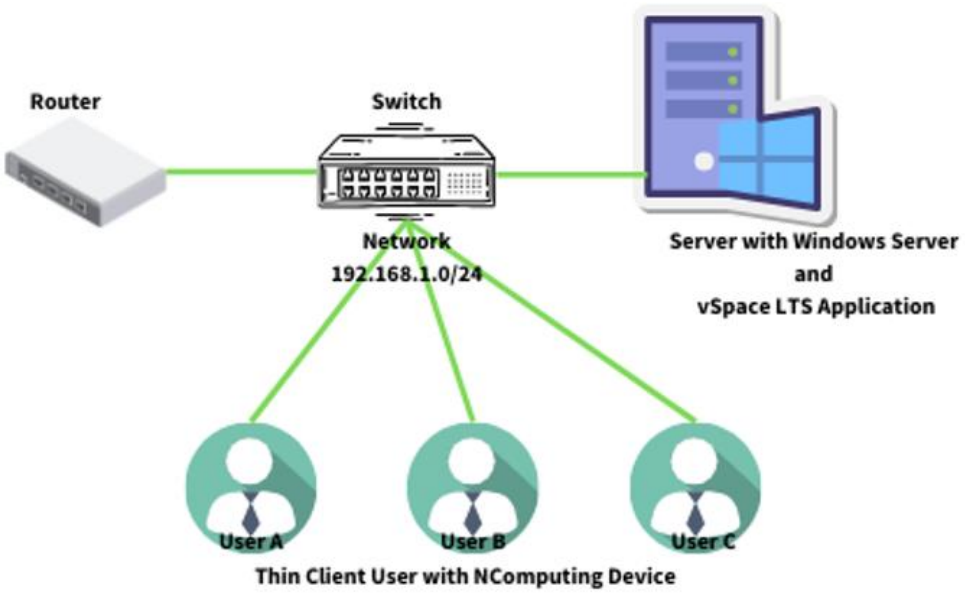
- **Monitoring Sistem:** Memantau aktivitas jaringan dan sistem untuk mendeteksi anomali dan potensi serangan.
- **Pembaruan Keamanan:** Secara rutin memperbarui perangkat lunak dan kebijakan keamanan untuk melindungi dari ancaman terbaru.
- **Backup dan Pemulihan:** Melakukan backup data secara berkala dan menguji rencana pemulihan untuk memastikan data dapat dipulihkan dengan cepat.
- **Pelatihan Berkelanjutan:** Memberikan pelatihan berkelanjutan kepada pengguna dan staf IT tentang praktik keamanan terbaru dan penggunaan sistem.

Berdasarkan peenjelasan tahapan NDLC tersebut pada subjek penelitian dapat dibuatkan sebagai berikut, yaitu dimana beberapa terminal Thin Client yang terhubung ke sebuah server yang menjalankan sistem operasi Windows Server dan berfungsi sebagai Domain Controller dengan Active Directory[14]. Untuk perangkat Thin Client yang digunakan adalah NComputing dimana pada server di sistem operasi Windows Server tersebut juga terpasang aplikasi controller vSpace LTS dari NComputing [12]. Untuk topologi jaringan yang digunakan adalah sebagai berikut:

This work is licensed under a Creative Commons Attribution 4.0 International License.
http://journal.stmikjayakarta.ac.id/index.php/JMIJayakarta

Jurnal Manajemen Informatika Jayakarta
Volume 4, Nomor 3, Juli 2024: halaman 258-265
P-ISSN: 2746-5985
e-ISSN: 2797-0930

DOI: https://doi.org/10.52362/jmijayakarta.v4i3.1531



Gambar 1. Topologi Jaringan Integrasi Thin Client dengan Domain Controller
Penjelasan pada gambar 1 sebagai berikut:

Penjelasan untuk topologi jaringan tersebut adalah sebagai berikut,

- **Server :** Server menjalankan Windows Server dan berfungsi sebagai Domain Controller dengan Active Directory. Server bertanggung jawab untuk mengatur otentikasi pengguna, manajemen kebijakan jaringan, dan pengelolaan sumber daya seperti file, printer, dan aplikasi. Active Directory menyimpan semua informasi pengguna dan komputer dalam jaringan, termasuk informasi otentikasi, kebijakan grup, dan atribut pengguna. vSpace server memanajemen perangkat dan pengguna Thin Client dalam hal ini NComputing yang terhubung ke server ini.
- **Thin Client User:** Merupakan perangkat fisik yang terhubung ke server melalui jaringan lokal (LAN) atau kita dapat sebutkan sebagai terminal. Terminal-terminal ini berfungsi sebagai klien, dan mereka menggunakan sumber daya yang disediakan oleh server. Pengguna mengakses aplikasi dan data melalui terminal ini, dan semua proses komputasi terjadi di server.
- **Switch (LAN):** Switch digunakan untuk menghubungkan semua perangkat dalam jaringan lokal (LAN), termasuk terminal dan server. Ini menyediakan konektivitas jaringan yang diperlukan untuk mengirim data antara perangkat dalam jaringan.
- **Router (Internet Gateway):** Router berfungsi sebagai gateway untuk menghubungkan jaringan lokal (LAN) dengan jaringan luas (WAN), seperti internet. Ini memungkinkan akses internet untuk terminal dan server, serta memfasilitasi komunikasi dengan jaringan eksternal lainnya.

Dengan menggunakan topologi jaringan ini, organisasi dapat mengimplementasikan infrastruktur yang efisien dan aman, memungkinkan pengguna untuk mengakses sumber daya dengan mudah dan memungkinkan administrator untuk mengelola jaringan dengan efisien menggunakan Domain Controller. Kami membuat kebijakan penggunaan akses internet dan jaringan lokal berdasarkan kebijakan penggunaan jaringan dan komputer sebagai berikut:

This work is licensed under a Creative Commons Attribution 4.0 International License.
http://journal.stmikjayakarta.ac.id/index.php/JMIJayakarta

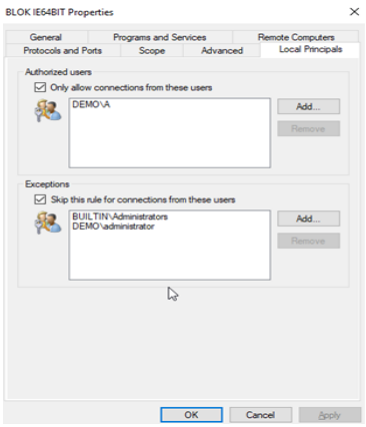
Jurnal Manajemen Informatika Jayakarta
Volume 4, Nomor 3, Juli 2024: halaman 258-265
P-ISSN: 2746-5985
e-ISSN: 2797-0930
DOI: https://doi.org/10.52362/jmijayakarta.v4i3.1531

Tabel 1. Kebijakan Penggunaan Jaringan & Komputer

No	User / Device / Terminal	IP Address	Akses Internet	Akses Printer	Akses USB
1	Router	**192.168.1.1/24**	**V**	**-**	**-**
2	Server	**192.168.1.200/24**	**V**	**V**	**V**
3	User A / Terminal A	**192.168.1.10/24**	**-**	**V**	**V**
4	User B / Terminal B	**192.168.1.11/24**	**V**	**V**	**-**
5	User C / Terminal C	**192.168.1.12/24**	**-**	**-**	**-**

Penjelasan dari Tabel 1. yaitu langkah pertama adalah mengaktifkan Domain Controller dimana diperlukan serangkaian langkah yang melibatkan instalasi dan konfigurasi Windows Server, pemasangan peran Active Directory Domain Services (AD DS), dan konfigurasi domain. Langkah kedua adalah memasang aplikasi vSpace LTS yang dapat diunduh dari website resmi NComputing dengan mendaftar gratis sebagai member terlebih dahulu. Pastikan kedua sistem tersebut telah berjalan secara otomatis di sistem operasi Windows, selain langkah diatas diperlukan juga lisensi Windows Server CAL User sebanyak jumlah terminal aktif yang digunakan[1]. Kemudian, pada Active Directory User & Computer buatlah user baru dengan pengaturan group pada Users dan Remote Desktop Users agar terminal Thin Client dapat masuk ke server Domain Controller menggunakan user yang dibuat tersebut. Setelah terminal berhasil terhubung dengan server Domain Controller saatnya menerapkan kebijakan yang dibuat pada tabel 1 sebelumnya dimana akses apa saja yang dibolehkan dan tidak oleh user tersebut, berikut penjelasannya

Kebijakan penggunaan akses internet dalam organisasi [3] sangat penting untuk menjaga keamanan informasi, produktivitas, dan ketersediaan sumber daya TI. Dengan merancang kebijakan penggunaan internet yang jelas dan diterapkan secara konsisten, perusahaan dapat menjaga keamanan informasi, meningkatkan produktivitas, dan meminimalkan risiko hukum yang terkait dengan penggunaan internet di lingkungan kerja. Pada Thin Client, akses internet tidak dapat dibatasi dengan menggunakan manajemen router [4] saja dikarenakan router hanya merekam aktivitas jaringan internet dari server Domain Controller saja, sedangkan pada perangkat Thin Client hanya terdeteksi sebagai aktiftas jaringan lokal seperti biasa saja. Ini disebabkan Thin Client menggunakan satu sumber pada server untuk beroperasi melalui protokol remote desktop, sehingga apapun perangkat Thin Client yang terhubung di jaringan lokal pada sisi user yang aktif dan terhubung ke server tetap menggunakan ip address dari server tersebut. Cara untuk menjalankan kebijakan ini adalah dengan menggunakan fitur firewall [9] dengan memblokir pemakaian aplikasi peramban pada server Domain Controller disisi outbond sehingga memberikan restricted pada user untuk mengakses internet dalam hal ini yang boleh memakai internet hanya User B sedangkan lainnya tidak bisa.



Gambar 2. Konfigurasi Firewall di Server Domain Controller untuk Memblokir Pemakaian Aplikasi Peramban Pada User Tertentu

This work is licensed under a Creative Commons Attribution 4.0 International License.
http://journal.stmikjayakarta.ac.id/index.php/JMIJayakarta

Jurnal Manajemen Informatika Jayakarta
Volume 4, Nomor 3, Juli 2024: halaman 258-265
P-ISSN: 2746-5985
e-ISSN: 2797-0930

DOI: https://doi.org/10.52362/jmijayakarta.v4i3.1531

Pada gambar 2 merupakan konfigurasi dengan membatasi User A agar tidak dapat menggunakan peramban untuk mengakses internet dan memberikan akses penuh kepada administrator untuk dapat mengakses internet melalui perambang.

Kebijakan printer sharing dalam organisasi [5] adalah seperangkat aturan dan prosedur yang mengatur cara penggunaan dan manajemen printer bersama di lingkungan kerja. Hal ini bertujuan untuk meningkatkan efisiensi penggunaan printer, menjaga keamanan informasi, dan memastikan sumber daya printer digunakan secara tepat. Untuk dapat mengakses printer pada terminal Thin Client, langkah pertama hubungkan terlebih dahulu printer pada salah satu terminal Thin Client, kemudian lakukan instalasi driver printer pada server Domain Controller dan kemudian pada pengaturan keamanan printer berikan akses user siapa saja yang dapat menggunakan printer tersebut dalam hal ini User A dan User B.

Kebijakan akses USB di organisasi [7] adalah seperangkat aturan dan prosedur yang mengatur penggunaan perangkat USB di lingkungan kerja. Hal ini bertujuan untuk melindungi keamanan informasi, mencegah kebocoran data, dan menjaga kepatuhan terhadap peraturan dan kebijakan organisasi. Untuk manajemen pemakaian USB ke terminal tertentu dapat dilakukan melalui konfigurasi dari domain controller atau dengan aplikasi host server bawaan terminal itu sendiri.

Dengan dijalankan kebijakan tersebut berdasarkan NDLC dapat membantu perusahaan atau organisasi mengoptimalkan penggunaan thin client dengan domain controller untuk mencapai tujuan bisnis mereka dengan aman dan efisien.

5 Kesimpulan

Pengembangan Keamanan Komputer dengan Teknologi Thin Client dan Domain Controller Dengan Metode Network Development Life Cycle (NDLC) adalah langkah yang potensial dalam meningkatkan efisiensi operasional dan keamanan sistem jaringan. beberapa aspek penting dalam meningkatkan keamanan dengan otentikasi pengguna, manajemen kebijakan grup, pemantauan aktivitas, dan segmentasi jaringan. Memudahkan membuat kebijakan untuk user yang terhubung dengan server domain controller seperti membuat kebijakan akses internet, kebijakan akses printer, dan kebijakan penggunaan akses USB yang tidak bisa dilakukan oleh manajemen router dikarenakan menggunakan protokol remote desktop. Dengan pendekatan yang tepat, organisasi dapat mengoptimalkan penggunaan teknologi ini untuk mencapai tujuan bisnis mereka dengan aman dan efisien[15].

Referensi (Reference)

[1] D. A. Zakoldaev, A. V. Gurjanov, A. V. Shukalov dan I. O. Zharinov, “Client-server technologies at the enterprises of Industry 4.0,” IOP Conf. Series: Materials Science and Engineering, 2019.

[2] Y. W, Yuliadi, S. Esabella dan Y. B. Fitriana, “Analisis Keamanan Jaringan Menggunakan Metode Security Policy Development Life Cycle (SPDLC),” KLIK: Kajian Ilmiah Informatika dan Komputer, pp. 634-641, 2023.

[3] S. Syed, H. Singh, S. K. Thangaraju, N. E. Bakri, K. Y. Hwa dan P. a. Kusalavan, “The Impact of Cyberloafing on Employees’ Job Performance: A Review of Literature,” Journal of Advances in Management Sciences & Information Systems, pp. 16-28, 2020.

[4] Solihin, E. Krisnaningsih, S. Dwiyatno, A. D. Jubaed, Y. F. Maulana dan Suhardianto, “MANAJEMEN AKSES INTERNET BERBASIS LIMITASI MENGGUNAKAN MIKHMON DAN ROUTER MIKROTIK,” Jurnal PROSISKO, pp. 84-91, 2023.

[5] Z. Sembiring, “Stuxnet Threat Analysis in SCADA (Supervisory Control And Data Acquisition) and PLC (Programmable Logic Controller) Systems,” Journal of Computer Science, Information Technologi and Telecommunication Engineering (JCoSITTE), pp. 96-103, 2020.

This work is licensed under a Creative Commons Attribution 4.0 International License.
http://journal.stmikjayakarta.ac.id/index.php/JMIJayakarta

P-ISSN: 2746-5985
e-ISSN: 2797-0930

DOI: https://doi.org/10.52362/jmijayakarta.v4i3.1531

[6] T. Sanjaya dan D. Setiyadi, "Network Development Life Cycle (NDLC) Dalam Perancangan Jaringan Komputer Pada Rumah Shalom Mahanaim," JURNAL MAHASISWA BINA INSANI, pp. 1-10, 2019.

[7] Prakasa dan J. E. Wahyu, "Peningkatan Keamanan Sistem Informasi Melalui Klasifikasi Serangan Terhadap Sistem Informasi," Jurnal Ilmiah Teknologi Informasi Asia, pp. 75-84, 2020.

[8] A. Naim, "New Trends in Business Process Management: Applications of Green Information Technologies," British Journal of Environmental Studies, pp. 12-23, 2021.

[9] Microsoft, "Windows Firewall overview," 22 11 2023. [Online]. Available: https://learn.microsoft.com/en-us/windows/security/operating-system-security/network-security/windows-firewall/.

[10] Microsoft, "Securing Domain Controllers Against Attack," 30 05 2024. [Online]. Available: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/securing-domain-controllers-against-attack.

[11] G. McDonald, P. Papadopoulos, N. Pitropakis, J. Ahmad dan W. J. Buchanan, "Ransomware: Analysing the Impact on Windows Active," Sensors, 2022.

[12] Y. Kristiyanto dan Sugiyono, "Pengembangan Jaringan Untuk Memperbaharui Sistem NComputing Versi Lawas ke Versi Terbaru Dengan Metode SDLC," INFORMATION MANAGEMENT FOR EDUCATORS AND PROFESSIONALS, pp. 71-80, 2023.

[13] Hariyanto, "Strategi Penerapan Green Computing Pada Unit Pengelola Sistem Informasi Pembelajaran Berdasarkan Metode Pendekatan Analytic Network Process(ANP): Studi Kasus SMPN 109 Jakarta," Jurnal Riset Komputer (JURIKOM), pp. 365-373, 2019.

[14] Haeruddin dan B. F. Pangaribuan, "PERANCANGAN DAN IMPLEMENTASI ACTIVE DIRECTORY DOMAIN CONTROLLER MENGGUNAKAN WINDOWS SERVER 2012 R2 DI PT. FLEXTRONICS TECHNOLOGY INDONESIA," Prosiding National Conference for Community Service Project (NaCosPro), pp. 1150-1154, 2021.

[15] P. Y. R. Grevisse, K. M. Hélène, T. T. Rufin, A. K. Gloire, K. S. David-Jackson, S. S. Albert, K. K. Chappelle dan G. S. Moïse, "Optimizing User and Resource Management in Modern Businesses Using a Domain Controller in Windows Server 2019," European Journal of Computer Science and Information Technology, pp. 26-55, 2024.

This work is licensed under a Creative Commons Attribution 4.0 International License.
http://journal.stmikjayakarta.ac.id/index.php/JMIJayakarta