Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 10, Nomor 1, Januari 2026
http://doi.org/10.33395/remik.v10i1.15912
e-ISSN : 2541-1330
p-ISSN : 2541-1332

Pendekatan Preventive Security dalam Optimalisasi Keamanan Sistem Operasi Windows

Syamsul Bahri
Universitas Pertiwi, Jakarta, Indonesia
syamsul.bahri@pertiwi.ac.id

*Penulis Korespondensi
Diajukan : 21/01/2026
Diterima : 12/02/2026
Dipublikasi : 15/02/2026

ABSTRACT

The Windows operating system is one of the most widely used computing platforms across various sectors, making it a primary target for security threats such as malware attacks, data breaches, and cyber intrusions. These high risks require the implementation of security strategies that are not only reactive but also preventive. This study aims to analyze the application of a preventive security approach in optimizing Windows operating system security through password management, antivirus utilization, and regular system patching and updating. The research employs a descriptive qualitative method based on literature review and observation of security implementation practices within Windows environments. Data were collected through the examination of scientific references, technical documentation, and direct observation of system security configurations. The results indicate that the implementation of integrated preventive security strategies significantly enhances system protection, reduces malware risks, and ensures the integrity and confidentiality of user data. Furthermore, user awareness of basic security practices plays a crucial role in improving overall system security effectiveness. This study concludes that preventive security is an effective and relevant approach for optimizing Windows operating system security and should be continuously applied as part of user information security management.

Keywords: *Antivirus, Patch Update, Preventive Security, System Security, Windows*

ABSTRAK

Sistem operasi Windows merupakan platform yang paling banyak digunakan oleh pengguna komputer di berbagai sektor, sehingga menjadi target utama berbagai ancaman keamanan seperti malware, pencurian data, dan serangan siber. Tingginya risiko tersebut menuntut penerapan strategi keamanan yang tidak hanya bersifat reaktif, tetapi juga preventif. Penelitian ini bertujuan untuk menganalisis penerapan pendekatan preventive security dalam optimalisasi keamanan sistem operasi Windows melalui pengelolaan password, penggunaan antivirus, serta penerapan patch dan update sistem secara berkala. Metode penelitian yang digunakan adalah deskriptif kualitatif dengan pendekatan studi literatur dan observasi terhadap praktik implementasi keamanan pada lingkungan sistem operasi Windows. Data dikumpulkan melalui kajian referensi ilmiah, dokumentasi teknis, serta pengamatan terhadap konfigurasi keamanan sistem. Hasil penelitian menunjukkan bahwa penerapan strategi keamanan preventif yang terintegrasi mampu meningkatkan perlindungan sistem secara signifikan, mengurangi potensi serangan malware, serta menjaga integritas dan kerahasiaan data pengguna. Selain itu, kesadaran pengguna terhadap praktik keamanan dasar juga berperan penting dalam efektivitas perlindungan sistem. Penelitian ini menyimpulkan bahwa pendekatan preventive security merupakan strategi yang efektif dan relevan dalam optimalisasi keamanan sistem operasi Windows, serta perlu diterapkan secara berkelanjutan sebagai bagian dari manajemen keamanan informasi pengguna.

Kata kunci : Antivirus, Keamanan Sistem, Preventive Security, Patch Update, Windows

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 10, Nomor 1, Januari 2026
http://doi.org/10.33395/remik.v10i1.15912
e-ISSN : 2541-1330
p-ISSN : 2541-1332

I. PENDAHULUAN

Perkembangan teknologi informasi telah mendorong penggunaan komputer secara luas di berbagai sektor, mulai dari pendidikan, pemerintahan, bisnis, hingga aktivitas personal sehari-hari. Dalam operasionalnya, sistem operasi berperan sebagai komponen utama yang mengendalikan seluruh sumber daya perangkat keras dan perangkat lunak agar dapat berfungsi secara optimal. Salah satu sistem operasi yang paling banyak digunakan secara global adalah Windows, karena memiliki antarmuka yang mudah digunakan, kompatibilitas tinggi terhadap berbagai aplikasi, serta dukungan pengembangan yang luas.

Namun, tingginya tingkat penggunaan sistem operasi Windows juga menjadikannya sebagai salah satu target utama serangan keamanan siber. Berbagai ancaman seperti malware, ransomware, phishing, pencurian data, serta eksploitasi celah sistem seringkali terjadi akibat lemahnya pengelolaan keamanan pada sisi pengguna. Tidak sedikit kasus kerusakan sistem dan kebocoran data yang disebabkan oleh kelalaian pengguna dalam menerapkan praktik keamanan dasar, seperti penggunaan password yang lemah, tidak melakukan pembaruan sistem, serta tidak memanfaatkan perangkat lunak keamanan secara optimal.

Upaya peningkatan keamanan sistem operasi selama ini cenderung bersifat reaktif, yaitu dilakukan setelah terjadinya gangguan atau serangan. Pendekatan tersebut dinilai kurang efektif dalam menghadapi ancaman siber yang semakin kompleks dan berkembang secara cepat. Oleh karena itu, diperlukan pendekatan keamanan yang bersifat preventif, yaitu dengan menerapkan langkah-langkah pencegahan sebelum terjadinya gangguan sistem. Pendekatan preventive security menekankan pada penguatan sistem melalui pengelolaan akses pengguna, perlindungan perangkat lunak, serta pembaruan sistem secara berkelanjutan.

Beberapa penelitian sebelumnya menunjukkan bahwa penerapan strategi keamanan preventif dapat secara signifikan menurunkan tingkat kerentanan sistem dan meningkatkan perlindungan data pengguna. Namun, kajian yang secara khusus membahas integrasi penerapan manajemen password, penggunaan antivirus, serta mekanisme patch dan update dalam konteks optimalisasi keamanan sistem operasi Windows masih terbatas. Kondisi ini menunjukkan adanya kesenjangan penelitian yang perlu dikaji lebih lanjut.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk menganalisis penerapan pendekatan preventive security dalam optimalisasi keamanan sistem operasi Windows melalui pengelolaan password, penggunaan antivirus, serta penerapan patch dan update sistem. Hasil penelitian diharapkan dapat memberikan kontribusi dalam pengembangan pemahaman mengenai strategi keamanan preventif yang efektif, serta menjadi referensi bagi pengguna dalam meningkatkan perlindungan sistem dan keamanan data.

II. LANDASAN TEORI

Sistem Operasi dan Keamanan Sistem

Sistem operasi merupakan perangkat lunak inti yang berfungsi mengelola sumber daya perangkat keras dan perangkat lunak serta menyediakan layanan bagi program aplikasi. Menurut Silberschatz, Galvin, dan Gagne (2018), sistem operasi berperan sebagai pengendali utama dalam manajemen proses, memori, penyimpanan, dan keamanan sistem. Dalam konteks keamanan informasi, sistem operasi memiliki fungsi penting dalam menjaga kerahasiaan, integritas, dan ketersediaan data pengguna.

Microsoft Windows sebagai salah satu sistem operasi paling populer di dunia memiliki tingkat kerentanan yang relatif tinggi terhadap serangan siber. Hal ini disebabkan oleh luasnya basis pengguna serta kompleksitas sistem yang membuka peluang eksploitasi celah keamanan (Stallings, 2017). Oleh karena itu, pengelolaan keamanan sistem operasi menjadi faktor penting dalam melindungi data dan menjaga stabilitas sistem.

Konsep Preventive Security

Preventive security merupakan pendekatan keamanan yang berfokus pada pencegahan terjadinya serangan sebelum sistem mengalami gangguan. Menurut Whitman dan Mattord (2018), strategi keamanan preventif mencakup penerapan kebijakan akses, perlindungan perangkat lunak, serta pembaruan sistem secara

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 10, Nomor 1, Januari 2026
http://doi.org/10.33395/remik.v10i1.15912
e-ISSN : 2541-1330
p-ISSN : 2541-1332

berkala untuk meminimalkan risiko ancaman. Pendekatan ini dianggap lebih efektif dibandingkan pendekatan reaktif karena mampu mengurangi peluang eksploitasi sejak awal.

Dalam praktiknya, preventive security mencakup berbagai mekanisme seperti autentikasi pengguna yang kuat, penggunaan perangkat lunak keamanan, serta manajemen patch sistem. Penerapan strategi ini dapat meningkatkan ketahanan sistem terhadap serangan malware, peretasan, dan kebocoran data (Pfleeger & Pfleeger, 2015).

Manajemen Password sebagai Mekanisme Keamanan

Password merupakan metode autentikasi yang paling umum digunakan dalam sistem komputer. Menurut Bishop (2019), penggunaan password yang kuat dan dikelola dengan baik dapat secara signifikan mengurangi risiko akses tidak sah terhadap sistem. Password yang efektif harus memiliki kombinasi karakter kompleks, tidak mudah ditebak, serta diperbarui secara berkala.

Penelitian oleh Florêncio dan Herley (2017) menunjukkan bahwa kelemahan password merupakan salah satu penyebab utama terjadinya pelanggaran keamanan informasi. Oleh karena itu, manajemen password yang baik menjadi komponen penting dalam strategi preventive security.

Peran Antivirus dalam Keamanan Sistem

Antivirus merupakan perangkat lunak yang dirancang untuk mendeteksi, mencegah, dan menghapus malware dari sistem komputer. Menurut Ayofe dan Irwin (2010), antivirus bekerja menggunakan metode deteksi berbasis tanda tangan, analisis heuristik, dan pemantauan perilaku sistem. Kombinasi metode tersebut memungkinkan antivirus mengidentifikasi ancaman baik yang telah dikenal maupun yang baru muncul.

Penggunaan antivirus secara konsisten terbukti mampu menurunkan tingkat infeksi malware serta meningkatkan perlindungan data pengguna (Behl & Behl, 2016). Namun, efektivitas antivirus sangat bergantung pada pembaruan database secara berkala.

Patch dan Update Sistem sebagai Strategi Keamanan

Patch dan update merupakan mekanisme penting dalam menjaga keamanan sistem operasi. Menurut Behl dan Behl (2016), patch digunakan untuk memperbaiki celah keamanan dan bug sistem, sedangkan update berfungsi meningkatkan kinerja dan stabilitas sistem secara keseluruhan. Kegagalan dalam melakukan pembaruan sistem dapat menyebabkan kerentanan yang mudah dieksploitasi oleh penyerang.

Studi oleh Rescorla (2017) menegaskan bahwa sebagian besar serangan siber terjadi karena pengguna tidak menerapkan patch keamanan yang tersedia. Oleh karena itu, pembaruan sistem secara rutin menjadi bagian penting dari strategi preventive security.

III. METODE PENELITIAN

Jenis dan Pendekatan Penelitian

Penelitian ini menggunakan metode deskriptif kualitatif dengan pendekatan studi literatur dan observasi sistem. Metode deskriptif kualitatif dipilih karena penelitian bertujuan untuk memahami dan menganalisis penerapan pendekatan preventive security dalam optimalisasi keamanan sistem operasi Windows secara konseptual dan praktis. Pendekatan ini memungkinkan peneliti untuk menggambarkan fenomena keamanan sistem secara sistematis, faktual, dan akurat berdasarkan data yang diperoleh.

Objek Penelitian

Objek penelitian dalam studi ini adalah mekanisme keamanan pada sistem operasi Microsoft Windows, khususnya yang berkaitan dengan strategi keamanan preventif, meliputi:

1. Manajemen password sebagai kontrol autentikasi pengguna
2. Penggunaan perangkat lunak antivirus sebagai perlindungan sistem
3. Penerapan patch dan update sistem sebagai upaya penutupan celah keamanan

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 10, Nomor 1, Januari 2026
http://doi.org/10.33395/remik.v10i1.15912
e-ISSN : 2541-1330
p-ISSN : 2541-1332

Teknik Pengumpulan Data

Data dalam penelitian ini diperoleh melalui beberapa teknik, yaitu:

1. Studi Literatur
   Pengumpulan data dilakukan dengan menelaah berbagai sumber ilmiah seperti buku, jurnal, prosiding, dan dokumentasi teknis yang relevan dengan keamanan sistem operasi dan konsep preventive security. Studi literatur bertujuan untuk memperoleh landasan teoritis serta memahami praktik terbaik dalam pengelolaan keamanan sistem.
2. Observasi Sistem
   Observasi dilakukan terhadap konfigurasi keamanan pada sistem operasi Windows untuk mengidentifikasi penerapan fitur keamanan preventif, termasuk pengaturan password, penggunaan antivirus bawaan sistem, serta mekanisme patch dan update.
3. Dokumentasi
   Dokumentasi dilakukan dengan mengumpulkan data berupa panduan teknis, tangkapan layar konfigurasi sistem, serta catatan implementasi keamanan yang mendukung analisis penelitian.

Teknik Analisis Data

Analisis data dalam penelitian ini menggunakan teknik analisis deskriptif kualitatif, yang dilakukan melalui tahapan berikut:

1. Reduksi Data, yaitu proses seleksi dan penyederhanaan data yang relevan dengan fokus penelitian.
2. Penyajian Data, yaitu pengorganisasian data dalam bentuk deskripsi sistematis mengenai praktik keamanan preventif.
3. Penarikan Kesimpulan, yaitu interpretasi hasil analisis untuk mengidentifikasi efektivitas penerapan preventive security dalam meningkatkan keamanan sistem operasi Windows.

Kerangka Analisis Penelitian

Penelitian ini menggunakan kerangka analisis berbasis konsep preventive security, yang menitikberatkan pada tiga aspek utama, yaitu:

1. Penguatan autentikasi pengguna melalui manajemen password
2. Perlindungan sistem melalui penggunaan antivirus
3. Pencegahan eksploitasi celah sistem melalui patch dan update

Kerangka analisis ini digunakan untuk mengevaluasi sejauh mana penerapan strategi keamanan preventif mampu meningkatkan perlindungan sistem dan mengurangi risiko ancaman siber.

IV. PEMBAHASAN

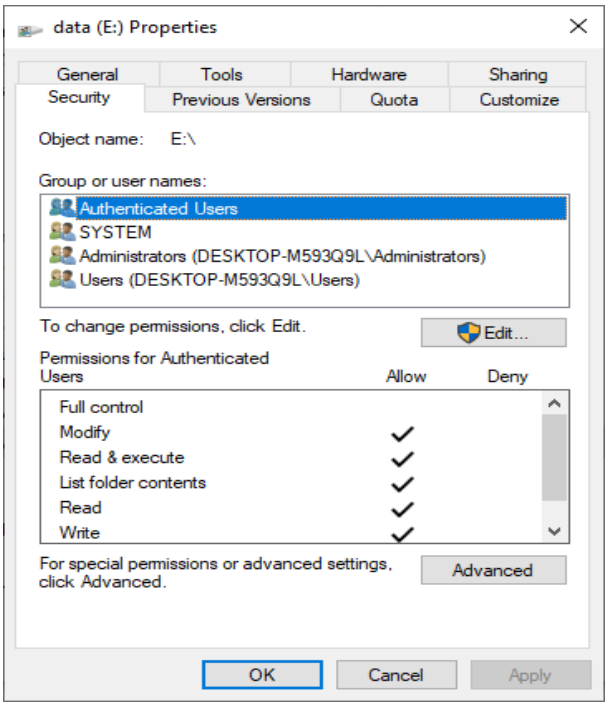
Implementasi Pendekatan Preventive Security pada Sistem Operasi Windows

Hasil kajian menunjukkan bahwa pendekatan preventive security pada sistem operasi Windows berfokus pada upaya pencegahan gangguan keamanan sebelum terjadinya serangan. Strategi ini menekankan pada penguatan sistem melalui kontrol akses, perlindungan perangkat lunak, serta pembaruan sistem secara berkelanjutan. Pendekatan preventif dinilai lebih efektif dibandingkan strategi reaktif karena mampu mengurangi peluang eksploitasi celah keamanan sejak awal (Whitman & Mattord, 2018).

Berdasarkan hasil observasi sistem, penerapan keamanan preventif pada Windows dapat diklasifikasikan ke dalam tiga mekanisme utama, yaitu manajemen password, penggunaan antivirus, serta penerapan patch dan update sistem.

Dalam meningkatkan mekanisme password diharuskan melakukan manajemen Group user yang digunakan untuk membagi sesuai dengan fungsinya.

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 10, Nomor 1, Januari 2026
http://doi.org/10.33395/remik.v10i1.15912
e-ISSN : 2541-1330
p-ISSN : 2541-1332



Gambar 1 Manajemen *Group user*

Pembagian group user tersebut adalah :

a. *Autenticated users*, mempunyai akses *modify, read & execute, list folder contents, read, and write*
b. *System*, mempunyai akses full control
c. *Administrators*, mempunyai akses full control
d. *Users*, mempunyai *akses read & execute, list folder contents,* dan *read*

Dalam grup user tersebut akan diketahui anggota masing-masing sesuai dengan fungsinya,

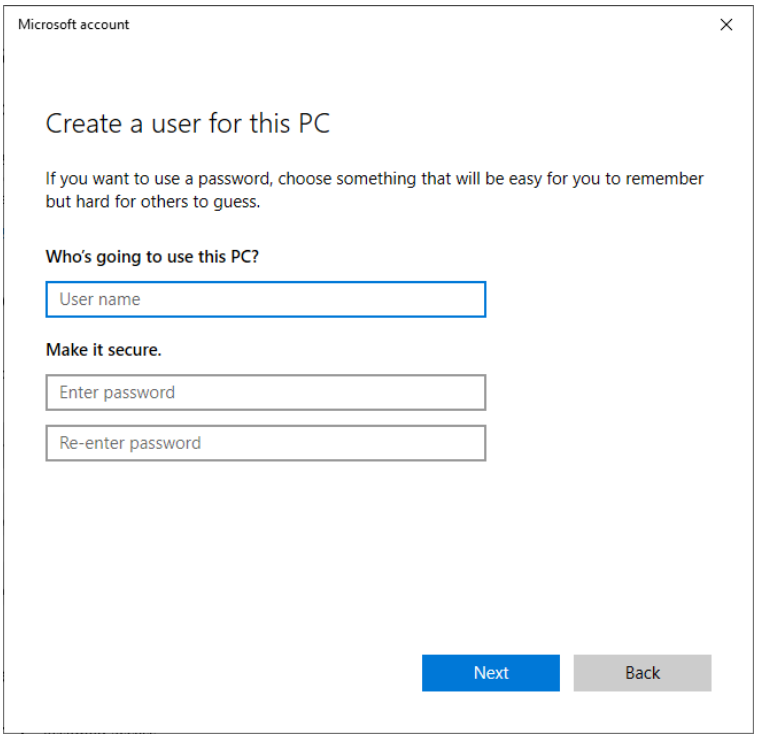
Analisis Manajemen Password sebagai Kontrol Autentikasi

Password merupakan lapisan keamanan pertama dalam sistem komputer yang berfungsi sebagai mekanisme autentikasi pengguna. Hasil penelitian menunjukkan bahwa pengelolaan password yang baik berkontribusi signifikan terhadap peningkatan keamanan sistem, khususnya dalam mencegah akses tidak sah.

Penggunaan password yang kompleks, kombinasi karakter, serta pembaruan secara berkala terbukti mampu menurunkan risiko pelanggaran keamanan. Temuan ini sejalan dengan penelitian Bishop (2019) yang menyatakan bahwa password yang lemah merupakan penyebab utama terjadinya pelanggaran keamanan informasi. Selain itu, studi Florêncio dan Herley (2017) juga menegaskan bahwa praktik penggunaan password yang tidak aman, seperti penggunaan ulang password, meningkatkan kerentanan sistem terhadap serangan siber.

Dengan demikian, manajemen password yang efektif menjadi komponen penting dalam penerapan strategi preventive security.

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 10, Nomor 1, Januari 2026
http://doi.org/10.33395/remik.v10i1.15912
e-ISSN : 2541-1330
p-ISSN : 2541-1332



Gambar 3 Pembuatan Akun User

Untuk meningkatkan keamanan dan mencegah akses tidak sah, kata sandi sebaiknya disusun menggunakan kombinasi huruf besar, angka, serta karakter khusus. Selain itu, hindari penggunaan informasi yang mudah ditebak, seperti tanggal lahir atau hal yang bersifat pribadi, dan disarankan untuk melakukan perubahan kata sandi secara berkala, minimal setiap tiga bulan sekali.

Efektivitas Antivirus dalam Perlindungan Sistem

Hasil observasi menunjukkan bahwa penggunaan perangkat lunak antivirus memberikan perlindungan signifikan terhadap ancaman malware. Antivirus bekerja melalui beberapa metode deteksi, seperti deteksi berbasis tanda tangan, analisis heuristik, dan pemantauan perilaku sistem secara real time.

Penelitian Ayofe dan Irwin (2010) menjelaskan bahwa kombinasi metode deteksi tersebut memungkinkan antivirus mengidentifikasi baik ancaman yang telah dikenal maupun malware baru yang belum memiliki pola serangan tetap. Selain itu, penggunaan antivirus yang diperbarui secara berkala terbukti mampu menurunkan tingkat infeksi malware serta menjaga integritas sistem (Behl & Behl, 2016).

Namun, hasil analisis juga menunjukkan bahwa efektivitas antivirus sangat bergantung pada kesadaran pengguna dalam melakukan pembaruan database secara rutin untuk mencegah, mendeteksi, dan memperbaiki sistem dan data yang rusak oleh virus. Dalam sistem operasi windows 10

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 10, Nomor 1, Januari 2026
http://doi.org/10.33395/remik.v10i1.15912
e-ISSN : 2541-1330
p-ISSN : 2541-1332

Gambar 4 Anti Virus

Cara kerja *antivirus* adalah :

a. Pendeteksian Berbasis Tanda Tangan (*Signature-Based Detection*)
   Antivirus menggunakan database tanda tangan virus untuk mengenali malware yang sudah diketahui sebelumnya. Ketika file diakses dan dimasukkan ke sistem, *antivirus* akan membandingkan dengan daftar tanda tangan tersebut, jika terjadi kecocokan maka file akan langsung dikarantina atau dihapus. Metode ini mempunyai kelemahan yaitu sangat tergantung pada *update* terbaru.
b. Analisa Heuristik (*Heuristic Analysis*)
   Cara ini digunakan untuk mendeteksi vrus baru yang belum terdeteksi sebelumnya, antvirus akan menganalisa struktur dan perilaku file untuk menentukan sesuatu yang mencurigakan. Cara ini bisa mendeteksi malware yang belum ada sebelumnya. Cara ini lebih efektif namun memiliki kesalahan deteksi yang lebih tinggi.
c. Analisis Berbasis Perilaku (*Behavioral Analysis*)
   Melalui cara ini antivirus memantau semua aktifitas aplikasi secara *real time* dan menilainya apakah perilakunya mencurigakan, hal ini termasuk mengakses file sistem mengenkripsi banyak *file* dalam waktu singkat, atau mengubah registri sistem. Ketika aktivitas tidak biasa terdeteksi, antivirus segera mengambil tindakan seperti memblokir, menghentikan proses, atau memberi peringatan.
d. Isolasi atau Karantina File
   Jika antivirus mendeteksi *file* yang mencurigakan sebagai potensi *malware*, *file* tersebut akan dipindahkan ke area karantina. Di sana, *file* tidak bisa dijalankan, dimodifikasi, maupun diakses oleh sistem, sehingga aman untuk dianalisis lebih lanjut oleh pengguna atau administrator sebelum dihapus atau dipulihkan.
e. Pembaruan Berkala
   Antivirus secara otomatis melakukan *updating* terhadap *database* tanda tangan virus dan modul proteksi lainnya. Ini sangat penting karena setiap hari muncul ribuan jenis *malware* baru. Antivirus yang tidak *update* akan menjadi usang dan tidak efektif terhadap ancaman terbaru.

Peran Patch dan Update dalam Menutup Celah Keamanan

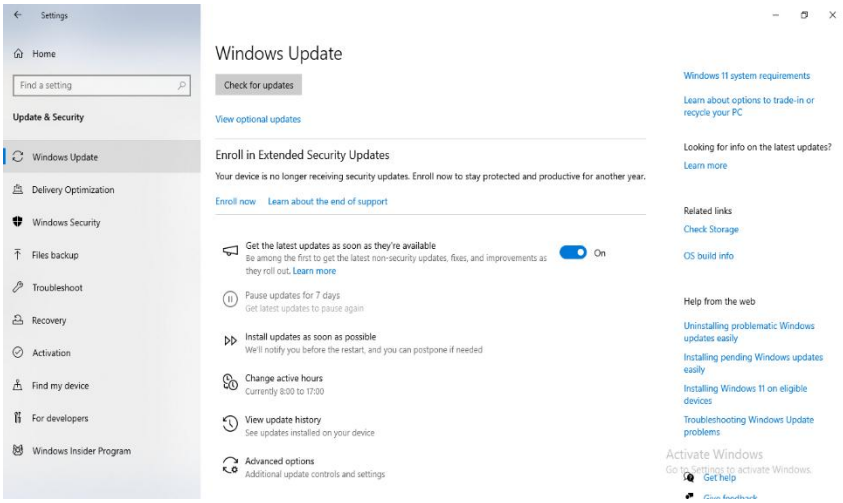
Patch dan update sistem merupakan mekanisme penting dalam menjaga keamanan sistem operasi. Hasil penelitian menunjukkan bahwa pembaruan sistem secara berkala mampu menutup celah keamanan yang berpotensi dieksploitasi oleh penyerang.

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 10, Nomor 1, Januari 2026
http://doi.org/10.33395/remik.v10i1.15912
e-ISSN : 2541-1330
p-ISSN : 2541-1332

Rescorla (2017) menyatakan bahwa sebagian besar serangan siber terjadi karena sistem tidak diperbarui, sehingga celah keamanan tetap terbuka. Selain itu, patch tidak hanya memperbaiki bug sistem, tetapi juga meningkatkan stabilitas dan kinerja sistem secara keseluruhan (Stallings, 2017).

Temuan penelitian ini menunjukkan bahwa pengguna yang secara rutin melakukan pembaruan sistem memiliki tingkat kerentanan keamanan yang lebih rendah dibandingkan pengguna yang mengabaikan proses patching.

Untuk melengkapi keamanan pada sistem operasi windows, maka harus selalu melakukan patch dan update. Patch adalah perbaikan kecil untuk memperbaiki *bug*, celah keamanan, atau masalah lainnya, sedangkan *update* adalah perbaikan besar untuk meningkatkan fungsionalitas, kinerja sistem, dan keamanan sistem.



Gambar 5 Windows Update

Integrasi Strategi Preventive Security

Hasil analisis menunjukkan bahwa penerapan preventive security secara terintegrasi memberikan dampak signifikan terhadap peningkatan keamanan sistem. Integrasi antara manajemen password, penggunaan antivirus, serta pembaruan sistem mampu menciptakan lapisan perlindungan berlapis (layered security).

Konsep ini sejalan dengan teori defense in depth yang menyatakan bahwa keamanan sistem akan lebih efektif apabila menggunakan beberapa mekanisme perlindungan secara bersamaan (Pfleeger & Pfleeger, 2015). Dengan pendekatan ini, kegagalan satu mekanisme keamanan tidak secara langsung menyebabkan kerusakan sistem secara keseluruhan.

Dampak Preventive Security terhadap Keamanan Sistem

Secara keseluruhan, hasil penelitian menunjukkan bahwa penerapan preventive security memberikan beberapa manfaat utama, yaitu:

1. Mengurangi risiko serangan malware
2. Meningkatkan perlindungan data pengguna
3. Menjaga stabilitas sistem
4. Mencegah akses tidak sah
5. Meningkatkan kesadaran keamanan pengguna

Temuan ini menunjukkan bahwa pendekatan preventive security merupakan strategi yang efektif dan relevan dalam optimalisasi keamanan sistem operasi.

V. KESIMPULAN

Penelitian ini bertujuan untuk menganalisis penerapan pendekatan preventive security dalam optimalisasi keamanan sistem operasi Windows melalui manajemen password, penggunaan antivirus, serta

e-ISSN : 2541-1330
p-ISSN : 2541-1332

penerapan patch dan update sistem. Berdasarkan hasil kajian literatur dan observasi implementasi keamanan sistem, dapat disimpulkan bahwa pendekatan preventive security terbukti efektif dalam meningkatkan perlindungan sistem terhadap berbagai ancaman keamanan siber.

Manajemen password yang baik mampu mengurangi risiko akses tidak sah melalui penerapan autentikasi yang kuat dan pengelolaan akses pengguna yang tepat. Penggunaan antivirus secara rutin dan terbarui berperan penting dalam mendeteksi serta mencegah penyebaran malware yang dapat merusak sistem dan mencuri data. Selain itu, penerapan patch dan update sistem secara berkala terbukti mampu menutup celah keamanan serta meningkatkan stabilitas dan kinerja sistem secara keseluruhan.

Hasil penelitian juga menunjukkan bahwa integrasi ketiga mekanisme keamanan tersebut menciptakan sistem perlindungan berlapis yang lebih efektif dibandingkan penerapan secara terpisah. Pendekatan preventive security tidak hanya berperan dalam mengurangi risiko serangan siber, tetapi juga meningkatkan kesadaran pengguna terhadap pentingnya praktik keamanan dasar dalam penggunaan sistem operasi. Dengan demikian, pendekatan preventive security dapat dinyatakan sebagai strategi yang relevan dan berkelanjutan dalam optimalisasi keamanan sistem operasi. Penerapan strategi ini secara konsisten diharapkan mampu meningkatkan perlindungan data, menjaga stabilitas sistem, serta mendukung terciptanya lingkungan komputasi yang lebih aman.

VI. REFERENSI

Ayofe, A. N., & Irwin, B. (2010). A survey of malware detection techniques. *IEEE Security & Privacy, 8*(2), 44–52.

Behl, A., & Behl, K. (2016). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.

Bishop, M. (2019). *Computer security: Art and science* (2nd ed.). Boston, MA: Addison-Wesley.

Florêncio, D., & Herley, C. (2017). Password reuse and security implications. *ACM Transactions on Information and System Security, 20*(3), 1–28.

Hidayat, R., & Prasetyo, Y. (2021). Analisis keamanan sistem informasi berbasis manajemen risiko teknologi informasi. *Jurnal Teknologi Informasi dan Ilmu Komputer, 8*(2), 245–252.

Kurniawan, D., & Nugroho, A. (2020). Implementasi keamanan jaringan komputer menggunakan metode layered security. *Jurnal Sistem Informasi, 16*(1), 33–41.

Mulyadi, M., & Sari, R. (2019). Evaluasi penerapan keamanan sistem informasi pada organisasi pendidikan. *Jurnal Informatika, 13*(2), 85–94.

Pfleeger, C. P., & Pfleeger, S. L. (2015). *Security in computing* (5th ed.). Upper Saddle River, NJ: Prentice Hall.

Pratama, I. P. A. E. (2018). Analisis ancaman keamanan sistem operasi pada lingkungan teknologi informasi modern. *Jurnal Nasional Teknologi dan Sistem Informasi, 4*(3), 120–128.

Rescorla, E. (2017). *Security engineering: A guide to building dependable distributed systems*. Indianapolis, IN: Wiley.

Setiawan, A., & Wibowo, S. (2022). Penerapan kebijakan keamanan informasi untuk meningkatkan perlindungan data pengguna. *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), 6*(1), 14–21.

Silberschatz, A., Galvin, P. B., & Gagne, G. (2018). *Operating system concepts* (10th ed.). Hoboken, NJ: Wiley.

Stallings, W. (2017). *Operating systems: Internals and design principles* (9th ed.). Boston, MA: Pearson.

Suryanto, T., & Rahmawati, D. (2023). Strategi preventive security dalam meningkatkan keamanan sistem komputer. *Jurnal Ilmiah Teknologi Informasi Asia, 17*(1), 55–64.

Whitman, M. E., & Mattord, H. J. (2018). *Principles of information security* (6th ed.). Boston, MA: Cengage Learning.

Yuliana, L., & Hartono, B. (2021). Analisis efektivitas penggunaan antivirus dalam perlindungan sistem komputer. *Jurnal Sistem dan Teknologi Informasi, 9*(3), 201–209.