JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

Mitigasi Serangan Ransomware Pada Sistem Operasi Windows Menggunakan Manajemen Patch Dan Firewall

Arya Mahisa Duta[1*], Muslim Gunawan [2], Muhammad Haikal [3], Ramza Nadra Syaf [4], Afkar Aulia[5*]
1,2,3,4,5 Program Studi Sistem Informasi Universitas Malikussaleh,Indonesia
Jl. Kampus Unimal Bukit Indah, Blang Pulo, Kec. Muara Satu, Kota Lhokseumawe, Aceh 24355 email:
[1]arya.240170013@gmail.com, [2]muslim.240170036@mhs.unimal.ac.id, [3]muhammad.240170011@mhs.unimal.ac.id,
[4]ramza.240170124@mhs.unimal.ac.id, [5]afkar.240170191@mhs.unimal.ac.id

ABSTRACT

Ancaman siber terus berevolusi seiring perkembangan teknologi, salah satunya adalah serangan Ransomware yang menyebabkan kerugian finansial yang signifikan dan mengganggu operasi bisnis serta individu. Kasus-kasus ransomware terkenal seperti WannaCry, NotPetya, GandCrab, Ryuk, dan REvil/Sodinokibi telah menunjukkan dampak negatif dari serangan tersebut. Insiden global WannaCry membuktikan bahwa celah keamanan sekecil apapun pada sistem operasi dapat berakibat fatal jika diabaikan. Penelitian ini bertujuan untuk meninjau kembali mekanisme serangan tersebut dan merumuskan langkah pertahanan praktis yang bisa diterapkan oleh pengguna Windows. Melalui pendekatan studi kasus dan kajian literatur teknis, ditemukan bahwa mayoritas infeksi terjadi akibat kelalaian dalam pemeliharaan sistem. Oleh karena itu, penerapan disiplin Manajemen Patch untuk menutup celah keamanan (vulnerability) dan konfigurasi Firewall untuk membatasi akses jaringan, terbukti menjadi metode mitigasi yang paling efektif dalam mencegah masuknya malware.

Kata Kunci: *Ransomware, Keamanan Cyber, Patch management, firewall, Windows.*

PENDAHULUAN

Dalam ekosistem digital, keamanan data bukan lagi sekadar pelengkap, melainkan kebutuhan mendasar. Namun, kesadaran pengguna komputer seringkali berbanding terbalik dengan risiko yang ada. Banyak pengguna yang masih mengabaikan peringatan pembaruan sistem operasi, padahal hal tersebut adalah garis pertahanan pertama melawan malware.

Salah satu jenis serangan yang paling merugikan adalah Ransomware. Berbeda dengan virus biasa yang mungkin hanya merusak sistem, Ransomware mengenkripsi data atau mengunci sistem korban, kemudian meminta tebusan agar akses bisa dipulihkan. Dalam beberapa tahun terakhir, serangan ini semakin marak dan tidak hanya menyasar perusahaan besar, tetapi juga individu dan usaha kecil. Salah satu contoh kasus ada pada serangan WannaCry pada tahun 2017, contoh nyata bagaimana sebuah malware bisa melumpuhkan infrastruktur di ratusan negara hanya dalam hitungan hari. Masalah utamanya bukan semata-mata pada kecanggihan virusnya, melainkan pada ribuan komputer yang dibiarkan memiliki celah keamanan terbuka.

Jurnal ini bertujuan untuk membedah kembali kasus tersebut sebagai bahan pembelajaran. Fokus utamanya adalah bagaimana kita, sebagai pengguna maupun administrator sistem, dapat mencegah kejadian serupa dengan memanfaatkan fitur keamanan yang sebenarnya sudah tersedia di Windows, yaitu manajemen update dan firewall.

KAJIAN LITERATUR

Ransomware

Ransomware adalah jenis perangkat lunak berbahaya yang digunakan oleh penjahat siber untuk membobol komputer dan kemudian mengenkripsi file sehingga orang yang berwenang tidak dapat mengaksesnya lagi. Setelah file dienkripsi, pelaku ancaman diberi ketentuan untuk membayar tebusan sebagai imbalan untuk kunci yang dapat mendekripsi file. Namun, dalam beberapa kasus, pelaku ancaman mungkin tetap tidak memberikan akses ke file bahkan setelah korban membayar tebusan.[1] Ada beberapa jenis ransomware, seperti:

- **Locker Ransomware:** Mengunci seluruh perangkat sehingga pengguna tidak dapat mengakses sistemnya. Meski begitu, Ransomware jenis ini tidak mengenkripsikan file atau folder korban.
- **Crypto Ransomware:** Mengenkripsi file penting di perangkat sehingga data tidak bisa dibuka. Setelah item dikunci dan dienkripsi, notifikasi akan muncul yang menyatakan bahwa Anda harus membayar sejumlah uang untuk membuka data yang dikunci.
- **Double Extortion Ransomware:** Ransomware yang menghancurkan file korban dan mengekstrak data dalam jumlah besar sebelum dienkripsi pada tahap akhir serangan. Selain mengenkripsi, pelaku juga mengancam akan membocorkan data korban jika tebusan tidak dibayar.[2]

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

Keamanan Data

Keamanan data merupakan upaya untuk melindungi data dari akses tidak sah, perubahan, atau perusakan. Ini mencakup banyak hal, seperti perangkat keras, perangkat lunak, perangkat penyimpanan, perangkat pengguna, kontrol akses dan administrasi serta kebijakan dan prosedur organisasi. Keamanan data juga sangat penting untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi (CIA Triad)[3]. Ada beberapa jenis data security, seperti :

- Encryption: metode pengamanan data melalui algoritma yang mengubah data menjadi sebuah format yang tidak akan terbaca oleh yang tidak memiliki wewenang.
- Authentication: Memastikan bahwa pihak yang mengakses data atau sistem adalah yang memiliki wewenang dan kredensialnya memang telah tercatat dalam database sistem tersebut.
- Access Control: membatasi akses baik secara fisik maupun digital yang menuju ke sistem, jaringan hingga data penting. Proses ini hanya akan memberi izin akses kepada pihak yang berwenang saja.
- Backup and Recovery: Jenis pengamanan yang paling wajib dilakukan, karena, jika terjadi kegagalan sistem, kerusakan, bencana atau kebocoran data, masih bisa memulihkan data dan mengakses sekaligus menggunakan data secara normal.
- Endpoint Protection: umum digunakan untuk melindungi perangkat akhir seperti smartphone dan komputer dari cyber crime. Pengamanan data jenis ini berupa perangkat lunak antivirus sekaligus perlindungan terhadap malware yang akan memantau dan mendeteksi tanda-tanda serangan cyber.
- Penghapusan Data: Menghapus data yang sudah tidak digunakan harus dilakukan dengan benar dan secara teratur. Penghapusan data dilakukan dengan menggunakan perangkat lunak dalam melakukan overwrite di perangkat penyimpanan supaya tidak dapat dipulihkan lagi. [4]

Data security merupakan dasar dalam upaya mitigasi ransomware, karena serangan ransomware menargetkan aspek confidentiality dan availability dari data. Dengan memahami data security, dapat membuat pengguna maupun administrator lebih aman dari ransomware.

Manajemen Patch

Manajemen patch adalah proses sistematis untuk mengidentifikasi, menguji, dan menerapkan pembaruan yang disebut patch pada perangkat lunak, sistem operasi, dan aplikasi dalam infrastruktur TI suatu organisasi. Ini merupakan aspek penting dari keamanan siber dan pemeliharaan TI[5]. Tujuan utamanya adalah menutup kerentanan yang diketahui, memperbaiki bug, dan meningkatkan stabilitas dan performa sistem untuk mengurangi risiko keamanan.

Gambar 1. Siklus Manajemen Patch

Patch yang diterapkan tepat waktu memainkan peran penting dalam mengurangi serangan ransomware. Banyak insiden ransomware dan eksploitasi lain berhasil karena kerentanan yang belum diperbaiki. Penerapan patch yang konsisten dan terencana mengurangi peluang eksploitasi zero-day atay eksploitasi yang cepat menyebar setekah adanya

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

kebocoran kode publik. Oleh karena itu, manajemen patch sering dimasukan sebagai komponen kunci dalam strategi pencegahan ransomware dan kebijakan keamanan cyber.

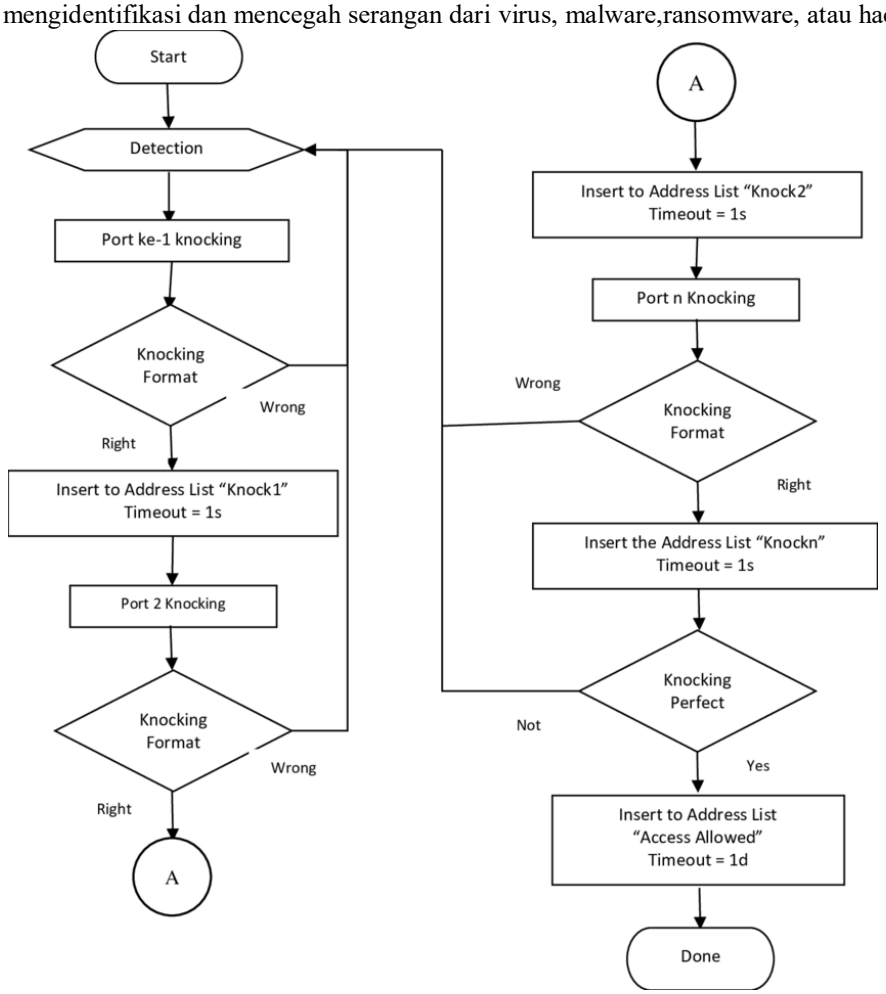
Ada beberapa hal yang bisa digunakan sebagai pedoman dasar praktik operasional manajemen patch, seperti:

- NIST SP 800-40 Rev.4: Panduan menyeluruh untuk perencanaan patch enterprise, meliputi identifikasi asset, prioritasasi patch berdasarjab dampak resiko, pengujian, serta pelaksanaan dan verifikasi patching. Panduan ini menekankan koordinasi lintas stakesholder dan pengurangan dampak operasional.[6]
- Panduan Vendor (mis. Microsoft): vendor besar seperti Microsoft menerbitkan kebijakan severity, indeks kemungkinan exploit, dan prosedur distribusi pembaruan (Patch Tuesday, OOB patches) yang penting bagi manajemen patch di Windows. Rekomendasi vendor seringkali menjadi dasar pengambilan Keputusan untuk penerapan patch.[7]

(*Prepare for a Ransomware Attack | Microsoft Learn*, n.d.; *Security Update Severity Rating System*, n.d.; Souppaya & Scarfone, n.d.)

Firewall

Firewall dalah sebuah sistem keamanan yang berfungsi untuk melindungi jaringan dan komputer dari ancaman yang datang dari luar. Firewall bekerja dengan menganalisis lalu lintas data yang masuk dan keluar jaringan, dan memfilter informasi yang masuk ke dalam jaringan. irewall juga dapat memantau dan mengontrol akses ke jaringan atau internet, serta mengidentifikasi dan mencegah serangan dari virus, malware,ransomware, atau hacker.[8]



Gambar 2. Firewall flowchart

Berdasarkan cara kerjanya, firewall dapat diklasifikasikan menjadi beberapa jenis. *Packet filtering firewall* melakukan penyaringan berdasarkan header paket tanpa memperhatikan isi data. *Stateful inspection firewall* mampu memantau status koneksi dan hanya mengizinkan paket yang merupakan bagian dari koneksi yang sah. Selain itu, terdapat *application-level gateway* atau *proxy firewall* yang melakukan inspeksi hingga lapisan aplikasi, sehingga memberikan tingkat keamanan yang lebih tinggi. Perkembangan terbaru juga menghadirkan *next-generation firewall*

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

(NGFW) yang menggabungkan fitur inspeksi aplikasi, *intrusion prevention system* (IPS), serta deteksi malware dalam satu sistem terintegrasi[9] (*8 Jenis-Jenis Firewall Untuk Keamanan Sistem Anda - Cloudmatika*, n.d.; *Pengertian Firewall Dalam Jaringan Komputer Dan Jenis-Jenisnya*, n.d.)

METODE PENELITIAN

Penulisan jurnal ini menggunakan metode studi literatur. Data dikumpulkan dari dokumentasi teknis Microsoft, laporan ransomware tentang dampak wannacry, serta materi perkuliahan Keamanan Sistem Komputer. Informasi yang didapat kemudian dianalisis untuk menghubungkan antara penyebab serangan (celah keamanan) dengan solusi teknis yang tersedia.

Tahapan pengumpulan data dilakukan dengan mengumpulkan artikel jurnal ilmiah, buku referensi, laporan teknis, serta dokumen dari berbagai organisasi dan vendor terkait keamanan digital. Tahapan penelitian diawali dengan penelusuran literatur yang didapatkan melalui berbagai sumber dan repositori karya ilmiah dengan menggunakan kata kunci ransomware, keamanan data, firewall, dan update patch. Sumber-sumber ini dipilih berdasarkan relevansi dan kredibilitasnya dalam memberikan informasi yang komprehensif dan terkini mengenai topik penelitian.

HASIL DAN PEMBAHASAN

Analisis Serangan: Mengapa Ransomware Bisa Masuk?

Ransomware bisa masuk ke dalam komputer pribadi dengan berbagai cara, seperti asal membuka Email yang berakhir dengan diarahkan ke dalam website palsu yang mengandung ransomware, mengunduh aplikasi bajakan maupun melalui celah keamanan pada sistem keamanan. Dalam kasus ransomware WannaCry, pelaku memanfaatkan celah dalam SMB Windows (EternalBlue). Eksploitasi ini bekerja dengan cara memindai internet atau jaringan lokal untuk mencari komputer yang port 445-nya terbuka dan masih menggunakan protokol SMBv1 yang rentan. SMB sendiri ialah protokol jaringan yang biasa digunakan windows untuk berbagi file. Pada kasus WannaCry, penyerang memanfaatkan kerentanan pada SMBv1.

Wannacry sendiri tergolong unik, karena ia bersifat wormable, yang berarti ia bisa menyebar sendiri secara otomatis melalui jaringan tanpa perlu pengguna lakukan apapun. Ketika target ditemukan, malware akan menyuntikkan dirinya ke dalam sistem. Proses ini terjadi di latar belakang tanpa sepengetahuan pengguna. Setelah berhasil masuk, barulah malware tersebut mengenkripsi file-file pengguna dan menampilkan pesan tebusan. Kecepatan penyebaran ini sangat masif karena sifatnya yang otomatis mencari korban baru dalam satu jaringan yang sama.

Langkah paling fundamental dalam mencegah Ransomware adalah memastikan sistem keamanan selalu diperbarui. Faktanya, jauh sebelum terjadinya kasus penyerangan WannaCry meledak, Microsoft sudah merilis patch keamanan dengan kode MS17-010. Patch keamanan ini melindungi mesin Windows dari kerentanan EternalBlue. Patch ini tersedia untuk Windows Vista; Windows 7, 8.1, 10; dan Windows Server 2008, 2008 R2, 2012, dan 2016. Sayangnya, fakta dilapangan menunjukan bahwa komputer yang terinfeksi adalah komputer yang tidak melakukan update patch keamanan.

Hal ini menujukan bahwa kegagalan manajemen patch dapat menjadi salah satu factor keberhasilan serangan ransomware. Oleh karena itu, manajemen patch sangat penting untuk mencegah ransomware kembali menyerang komputer pribadi. Untuk pengguna personal, dapat dengan mengaktifkan "Automatic Update" di Windows. Untuk administrator jaringan, penggunaan WSUS (Windows Server Update Services) diperlukan untuk memastikan seluruh komputer klien mendapatkan update keamanan tepat waktu sebelum celah tersebut dimanfaatkan peretas.

Selain dari manajemen patch, pertahanan lapis kedua untuk mencegah ransomware ialah Firewall. Meskipun sebuah sistem mungkin memiliki celah keamanan (belum sempat update patch), serangan dari jaringan luar bisa digagalkan jika pintu masuknya ditutup. Dalam kasus serangan berbasis SMB, Port 445 adalah pintu gerbang utamanya. Jika komputer tersebut tidak difungsikan sebagai file server publik, maka port ini wajib diblokir dari akses internet. Konfigurasi Windows Firewall harus disetel untuk menolak (drop) koneksi masuk ke port 445 dari IP yang tidak dikenal. Dengan demikian, meskipun ada malware yang mencoba masuk, ia akan tertahan di pintu masuk dan tidak bisa menyentuh sistem operasi.

KESIMPULAN

Berdasarkan analisis di atas, dapat disimpulkan bahwa keamanan sistem komputer tidak hanya bergantung pada antivirus, tetapi lebih kepada kedisiplinan pemeliharaan sistem. Insiden WannaCry dapat dijadikan pembelajaran bahwa membiarkan sistem keamanan pada komputer tidak diperbarui tidak ada bedanya membiarkan tidak mengunci gerbang rumah. Hanya tinggal menunggu waktu saja hingga pencuri dapat masuk dan mengancam pemilik rumah. Selain manajemen patch, firewall juga sangat berperan penting sebagai pertahanan tambahan yang penting dalam memitigasi ransomware. Kombinasi antara manajemen patch yang baik dan konfigurasi firewall yang tepat terbukti menjadi

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

strategi efektif dalam mengurangi risiko dan dampak serangan ransomware pada komputer pribadi maupun jaringan organisasi.

REFERENSI

[1] R. G. A. Asbath, Ilpan, R. P. Anugrah, and A. Setiawan, "Analisis Dampak Ransomware Pada Keamanan Data," *J. Kumpul. Ilmu Komput. Dan Perubahan Digit.*, vol. 1, no. 1, pp. 17–23, 2025.

[2] B. Hartono, "Ransomware: Memahami Ancaman Keamanan Digital," *Bincang Sains dan Teknol.*, vol. 2, no. 02, pp. 55–62, May 2023, doi: 10.56741/bst.v2i02.353.

[3] "Data Security: Definition, Importance, and Types | Fortinet." Accessed: Dec. 14, 2025. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/data-security

[4] "Data Security: Pengertian, Jenis Serta Kegunaanya untuk Keamanan Data." Accessed: Dec. 14, 2025. [Online]. Available: https://binus.ac.id/bandung/2024/02/data-security-pengertian-jenis-serta-kegunaanya-untuk-keamanan-data/

[5] "Apa Itu Manajemen Patch? Semua yang Perlu Anda Ketahui." Accessed: Dec. 19, 2025. [Online]. Available: https://www.enterprisenetworkingplanet.com/security/what-is-patch-management/

[6] M. Souppaya and K. Scarfone, "NIST Special Publication NIST SP 800-40r4 Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology", doi: 10.6028/NIST.SP.800-40r4.

[7] "Prepare for a ransomware attack | Microsoft Learn." Accessed: Dec. 14, 2025. [Online]. Available: https://learn.microsoft.com/en-us/azure/security/fundamentals/ransomware-prepare?utm_source=chatgpt.com

[8] "Pengertian Firewall dalam Jaringan Komputer dan Jenis-Jenisnya." Accessed: Dec. 14, 2025. [Online]. Available: https://it.telkomuniversity.ac.id/pengertian-firewall-dalam-jaringan-komputer-dan-jenis-jenisnya/

[9] "8 Jenis-jenis Firewall untuk Keamanan Sistem Anda - Cloudmatika." Accessed: Dec. 14, 2025. [Online]. Available: https://cloudmatika.co.id/blog-detail/jenis-jenis-firewall