# PENCEGAHAN RANSOMWARE BERBASIS EDUKASI PENGGUNA DAN TEKNOLOGI: TINJAUAN LITERATUR

**Ifnu Abdul Aziz Abdullah**

STMIK Samarinda

ifnuabdullah@gmail.com

**Abstrak**

Ransomware merupakan salah satu ancaman siber yang paling meresahkan dalam era digital saat ini. Serangan ini bekerja dengan cara mengenkripsi data milik korban dan meminta tebusan agar data tersebut dapat diakses kembali. Dampaknya tidak hanya merugikan secara finansial, tetapi juga dapat mengganggu operasional dan merusak reputasi suatu institusi. Artikel ini bertujuan untuk mengkaji berbagai strategi pencegahan ransomware melalui pendekatan studi literatur, dengan fokus pada dua pendekatan utama, yaitu edukasi pengguna dan penerapan teknologi. Dari berbagai sumber yang dikaji, ditemukan bahwa rendahnya literasi digital pengguna sering kali menjadi celah utama terjadinya serangan, terutama melalui email phishing dan praktik keamanan yang buruk. Oleh karena itu, peningkatan kesadaran serta pelatihan tentang keamanan siber sangat penting. Selain itu, penggunaan teknologi seperti firewall, sistem deteksi ancaman, backup data berkala, dan perangkat lunak antivirus yang mutakhir juga menjadi elemen penting dalam perlindungan sistem. Tinjauan ini menunjukkan bahwa kombinasi antara edukasi pengguna dan pemanfaatan teknologi secara tepat merupakan langkah efektif untuk mencegah serangan ransomware. Hasil kajian ini diharapkan dapat menjadi rujukan dalam membangun sistem keamanan informasi yang lebih tangguh dan adaptif di berbagai sektor.

**Kata Kunci:** ransomware, pencegahan ransomware, edukasi pengguna

**Abstract**

Ransomware is one of the most disturbing cyber threats in today's digital era. This attack works by encrypting the victim's data and demanding a ransom so that the data can be accessed again. The impact is not only financially detrimental, but can also disrupt operations and damage an institution's reputation. This article aims to examine various ransomware prevention strategies through a literature study approach, focusing on two main approaches, namely user education and technology implementation. From various sources reviewed, it was found that low digital literacy of users is often the main loophole for attacks, especially through phishing emails and poor security practices. Therefore, increasing awareness and training on cybersecurity is very important. In addition, the use of technology such as firewalls, threat detection systems, regular data backups, and up-to-date antivirus software are also important elements in system protection. This review shows that the combination of user education and proper use of technology is an effective step to prevent ransomware attacks. The results of this study are expected to be a reference in building a more resilient and adaptive information security system in various sectors.

**Keywords**: ransomware, ransomware prevention, user education

## PENDAHULUAN

Di tengah pesatnya perkembangan teknologi informasi dan komunikasi (TIK), dunia digital telah menjadi bagian integral dari kehidupan manusia, dari sektor bisnis hingga pendidikan, pemerintahan, dan bahkan kehidupan pribadi. Proses digitalisasi ini telah mempermudah banyak aktivitas manusia, memungkinkan peningkatan produktivitas, efisiensi, dan aksesibilitas yang sebelumnya sulit tercapai. Namun, semakin berkembangnya adopsi teknologi digital juga disertai dengan meningkatnya ancaman terhadap keamanan siber. Salah satu ancaman yang paling signifikan dan merusak dalam beberapa tahun terakhir adalah ransomware.(Kristalia & Wibisono, 2024)

Ransomware merupakan jenis malware yang dirancang untuk mengenkripsi data yang ada di perangkat korban, sehingga data tersebut menjadi tidak dapat diakses. Setelah berhasil mengenkripsi data, penyerang akan meminta sejumlah uang tebusan, biasanya dalam bentuk mata uang kripto seperti Bitcoin, dengan janji untuk memberikan kunci dekripsi yang diperlukan agar korban dapat mengakses data mereka kembali.(Ferdiansyah, 2018) Serangan ransomware ini telah menyebabkan kerugian finansial yang signifikan bagi individu, organisasi, bahkan lembaga pemerintah dan infrastruktur kritikal. Dampaknya sangat luas, mulai dari kerugian finansial, gangguan operasional, hingga kerusakan reputasi yang dapat berlangsung lama. Beberapa serangan bahkan mengancam stabilitas ekonomi dan sosial, dengan contoh nyata seperti serangan terhadap sistem rumah sakit, transportasi, dan sektor energi.(Wijanarko et al., 2023)

Penyebab utama dari maraknya serangan ransomware adalah kerentanannya sistem dan kelengahan pengguna. Sebagian besar serangan ransomware terjadi akibat ketidaktahuan atau kelalaian pengguna dalam mengenali ancaman, terutama dalam bentuk email phishing, lampiran berbahaya, dan link yang disusupi malware. Dalam banyak kasus, pengguna menjadi sasaran empuk bagi para penyerang yang memanfaatkan kelemahan ini untuk menyusup ke dalam sistem. Oleh karena itu, edukasi pengguna menjadi salah satu strategi yang sangat penting dalam mencegah terjadinya serangan ransomware. Meningkatkan kesadaran tentang cara-cara mendeteksi ancaman, serta pemahaman mengenai praktik keamanan yang baik, adalah langkah pertama yang dapat membantu memperkuat pertahanan terhadap serangan ini.(Susanto et al., 2023)

Namun, edukasi pengguna saja tidak cukup. Perkembangan ancaman yang semakin canggih membutuhkan solusi teknologi yang lebih tangguh dan proaktif. Teknologi-teknologi keamanan, seperti sistem deteksi dan pencegahan intrusi (IDS/IPS), firewall, enkripsi data, serta backup data yang teratur, adalah elemen-elemen penting dalam membangun pertahanan yang efektif. Penerapan teknologi yang tepat dapat membantu mendeteksi aktivitas mencurigakan, mencegah penyusupan, dan mengurangi dampak dari serangan ransomware. Dengan mengintegrasikan edukasi pengguna dengan penerapan teknologi yang sesuai, organisasi dapat menciptakan pertahanan ganda yang lebih solid untuk menghadapi serangan ransomware.(Hartono, 2023)

Artikel ini bertujuan untuk mengkaji pendekatan pencegahan ransomware melalui dua aspek utama, yakni edukasi pengguna dan penerapan teknologi yang tepat. Pendekatan ini bukan hanya mengandalkan satu sisi saja, tetapi menggabungkan faktor manusia dan teknologi untuk menciptakan sistem pertahanan yang lebih komprehensif dan efektif. Artikel ini disusun dengan pendekatan studi literatur untuk mengeksplorasi berbagai riset, temuan, dan praktik yang telah ada, guna memberikan wawasan yang lebih mendalam tentang bagaimana strategi ini dapat diterapkan secara optimal. Melalui tinjauan ini, diharapkan dapat ditemukan solusi yang lebih efektif untuk mengurangi dan mencegah serangan ransomware di masa depan, serta memberikan kontribusi pada pengembangan kebijakan dan prosedur yang dapat diterapkan oleh berbagai sektor.

## METODE

Artikel ini menggunakan pendekatan studi literatur (literature review) untuk menganalisis dan mengevaluasi berbagai penelitian dan temuan yang terkait dengan pencegahan serangan ransomware melalui edukasi pengguna dan penerapan teknologi yang tepat. Pendekatan studi literatur dipilih karena memungkinkan penulis untuk mengumpulkan, mengintegrasi, dan mengevaluasi informasi dari berbagai sumber yang relevan dan terkini dalam upaya mengidentifikasi solusi yang dapat diterapkan secara efektif dalam pencegahan ransomware. Metode ini juga memungkinkan penulis untuk menggali kesenjangan pengetahuan yang ada dan memberikan wawasan yang lebih komprehensif mengenai pendekatan yang lebih baik dalam mengurangi ancaman ransomware.

Metode ini penulis lakukan ada melakukan serangkaian tahapan sebagai berikut:

1. Identifikasi dan Pemilihan Sumber Literatur

Proses pertama dalam metode ini adalah identifikasi dan pemilihan sumber-sumber literatur yang relevan. Sumber-sumber yang digunakan dalam artikel ini mencakup berbagai publikasi ilmiah, artikel jurnal, buku, laporan penelitian, artikel berita, serta sumber-sumber teknis yang diterbitkan dalam kurun waktu 5–10 tahun terakhir. Pemilihan literatur difokuskan pada topik yang membahas dua aspek penting berupa pencegahan ransomware melalui edukasi pengguna dan teknologi yang diterapkan untuk mitigasi serangan ransomware. Sumber-sumber tersebut diperoleh melalui basis data seperti Google Scholar, IEEE Xplore, ScienceDirect,

SpringerLink, dan ACM Digital Library, serta dokumen dari organisasi terkait keamanan siber seperti NIST (National Institute of Standards and Technology) dan CERT (Computer Emergency Response Team).

Kriteria inklusi untuk literatur yang dipilih mencakup artikel yang berfokus pada riset, temuan, atau solusi yang terkait dengan pendidikan pengguna tentang keamanan siber, pencegahan malware, serta penerapan teknologi keamanan khususnya yang relevan dengan ransomware. Selain itu, artikel-artikel yang memuat analisis mengenai dampak serangan ransomware pada sektor-sektor kritikal seperti kesehatan, pendidikan, dan pemerintahan juga termasuk dalam kriteria pemilihan.

2. Analisis dan Kategorisasi Literatur

Setelah literatur terkumpul, langkah berikutnya adalah menganalisis dan mengategorikan informasi yang diperoleh. Literasi penelitian dibagi ke dalam dua kategori yakni:

a. Edukasi Pengguna untuk Pencegahan Ransomware, bagian ini akan mengkaji berbagai penelitian yang berfokus pada pentingnya peningkatan kesadaran dan edukasi pengguna dalam mencegah serangan ransomware. Beberapa tema yang dibahas dalam kategori ini meliputi strategi pelatihan pengguna, metode pencegahan yang berbasis pada perilaku, serta efektivitas program-program edukasi yang telah diterapkan di berbagai organisasi dan sektor. Penulis akan mengevaluasi pendekatan-pendekatan seperti simulasi phishing, penggunaan perangkat lunak keamanan yang mudah dipahami, serta pentingnya pengembangan kebijakan internal yang mengedepankan keselamatan data dan pelatihan berkelanjutan.
b. Penerapan Teknologi dalam Pencegahan Ransomware, kategori ini berfokus pada berbagai solusi teknologi yang diterapkan untuk memitigasi ancaman ransomware, seperti penggunaan sistem deteksi intrusi (IDS), sistem pencegahan intrusi (IPS), enkripsi data, backup yang terjadwal, serta pemanfaatan perangkat lunak antivirus dan antimalware yang dilengkapi dengan pemindaian berbasis AI untuk mendeteksi dan mencegah serangan ransomware. Penulis akan menilai berbagai alat teknologi dan platform yang telah terbukti efektif dalam melindungi data, serta mengurangi kemungkinan infeksi ransomware dalam infrastruktur digital.

3. Sintesis dan Penilaian Efektivitas Pendekatan yang Ada

Selanjutnya, informasi yang diperoleh dari literatur yang relevan akan disintesis untuk memberikan pemahaman yang lebih jelas tentang efektivitas kedua pendekatan tersebut, yaitu edukasi pengguna dan teknologi, dalam pencegahan serangan ransomware. Dalam sintesis ini, penulis akan menilai sejauh mana kombinasi antara upaya edukasi yang kuat dan teknologi yang handal dapat meningkatkan perlindungan terhadap sistem informasi, baik pada level individu, organisasi, maupun sektor kritikal. Selain itu, evaluasi akan dilakukan terhadap keberhasilan dan kekurangan dari pendekatan yang ada, termasuk faktor-faktor yang memengaruhi efektivitasnya. Misalnya, efektivitas program edukasi pengguna akan diukur berdasarkan pengurangan insiden serangan ransomware, sementara efektivitas teknologi akan dinilai berdasarkan kemampuan alat atau sistem dalam mencegah atau memitigasi dampak dari ransomware.

4. Pembahasan Tren dan Tantangan Terkini

Sebagai bagian dari metode ini, penulis juga akan membahas tren terbaru dalam pencegahan ransomware, termasuk teknologi yang sedang berkembang, serta perubahan dalam perilaku pengguna yang dapat mempengaruhi keberhasilan pencegahan. Misalnya, tren penggunaan blockchain dan kecerdasan buatan (AI) dalam mendeteksi ancaman yang lebih canggih akan dibahas, serta bagaimana tren ini dapat meningkatkan ketahanan terhadap serangan ransomware. Tantangan yang dihadapi dalam penerapan edukasi pengguna juga akan dikaji lebih dalam, seperti tingkat kesadaran yang rendah di kalangan pengguna, perbedaan dalam kemampuan teknis antar individu, dan ketergantungan pada teknologi yang kadang tidak efektif dalam menghadapi varian ransomware yang terus berkembang.

5. Pengembangan Rekomendasi dan Solusi Praktis

Akhirnya, berdasarkan hasil analisis dan sintesis literatur, artikel ini akan memberikan rekomendasi praktis mengenai pendekatan yang dapat diterapkan oleh berbagai organisasi dan institusi untuk mencegah serangan ransomware. Rekomendasi ini mencakup strategi yang menggabungkan edukasi pengguna secara efektif dengan penerapan teknologi yang canggih dan terintegrasi, serta kebijakan keamanan yang mendukung peningkatan kesadaran dan pengurangan risiko serangan..

## HASIL DAN PEMBAHASAN

Serangan ransomware, yang terus berkembang seiring dengan kemajuan teknologi, telah menjadi salah satu ancaman siber yang paling merusak di dunia digital. Dampaknya yang sangat besar, mulai dari kerugian finansial hingga gangguan operasional, menjadikannya sebagai topik yang sangat penting untuk dibahas, terutama dalam konteks pencegahan. Dalam artikel ini, membahas dua pendekatan utama untuk mencegah serangan ransomware, yaitu melalui edukasi pengguna dan penerapan teknologi yang tepat, serta menggali efektivitas keduanya berdasarkan hasil studi literatur yang ada.

1. Edukasi Pengguna, Kunci Utama dalam Pencegahan Ransomware

Salah satu faktor utama yang menyebabkan keberhasilan serangan ransomware adalah kelalaian pengguna dalam mengidentifikasi ancaman atau mengekspos data mereka melalui perilaku yang tidak hati-hati. Oleh karena

itu, edukasi pengguna memainkan peran yang sangat penting dalam mengurangi risiko serangan ransomware. Berdasarkan studi yang ada, banyak organisasi yang berhasil mengurangi insiden ransomware dengan menerapkan program pelatihan pengguna yang menyeluruh. Edukasi pengguna mencakup pemahaman tentang berbagai teknik serangan yang digunakan oleh pelaku kejahatan siber, seperti phishing, lampiran berbahaya, dan link yang disusupi malware. Salah satu pendekatan yang terbukti efektif adalah simulasi phishing, di mana pengguna diberikan pengalaman langsung dalam menghadapi email phishing dan diajarkan cara mengenali tanda-tanda dari email berbahaya. Selain itu, pelatihan yang berkelanjutan juga diperlukan, karena ancaman ransomware terus berkembang, sehingga pengetahuan pengguna harus selalu diperbarui. Penelitian oleh Kaspersky (2019) menunjukkan bahwa pelatihan yang dilakukan secara rutin dapat meningkatkan kesadaran pengguna mengenai keamanan siber dan mengurangi kemungkinan mereka untuk mengklik link berbahaya atau membuka lampiran yang terinfeksi. Bahkan, beberapa organisasi yang menerapkan simulasi serangan siber melaporkan penurunan jumlah serangan ransomware secara signifikan setelah karyawan mereka mengikuti pelatihan.(Community, 2019)

Namun, meskipun edukasi pengguna memiliki potensi besar dalam mengurangi risiko, tetap ada tantangan terkait dengan implementasinya. Salah satunya adalah perbedaan tingkat kesadaran antara pengguna dengan latar belakang teknis dan non-teknis. Pengguna yang kurang memahami teknologi atau tidak terbiasa dengan ancaman siber cenderung lebih rentan menjadi korban serangan. Oleh karena itu, pendekatan yang lebih personal dan disesuaikan dengan tingkat pemahaman individu perlu dipertimbangkan untuk mencapai efektivitas yang lebih tinggi.

2. Peran Teknologi dalam Pencegahan Ransomware

Sementara edukasi pengguna memberikan pendekatan berbasis manusia untuk mengurangi risiko ransomware, teknologi memainkan peran yang tak kalah penting dalam pencegahan serangan ini. Penggunaan teknologi yang tepat dapat membantu mendeteksi dan mencegah ancaman ransomware sebelum mencapai sistem yang lebih besar. Berbagai teknologi telah dikembangkan untuk membantu melindungi sistem dari serangan ransomware, termasuk perangkat lunak antivirus, sistem deteksi dan pencegahan intrusi (IDS/IPS), enkripsi data, serta pencadangan data yang rutin. Misalnya, antivirus dan antimalware yang terus diperbarui mampu mendeteksi tanda-tanda ransomware sejak dini, sebelum ia dapat mengenkripsi data atau menyebar ke sistem lainnya. Selain itu, penggunaan sistem firewall yang kuat juga penting untuk membatasi akses jaringan dari sumber yang tidak sah.(Brunnstein, 1999)

Enkripsi data, baik dalam bentuk file maupun komunikasi, juga memainkan peran penting dalam mengurangi risiko kerugian data akibat serangan ransomware. Dengan enkripsi, meskipun data berhasil terinfeksi dan dienkripsi oleh pelaku serangan, data tersebut akan tetap aman dan tidak dapat dibaca tanpa kunci enkripsi yang tepat. Ini memberikan lapisan perlindungan tambahan, sehingga meskipun tebusan diminta, data korban tidak dapat dipergunakan oleh pelaku. Pencadangan data yang terjadwal dan terpisah dari sistem utama juga menjadi strategi yang efektif dalam mencegah kerugian besar akibat ransomware. Dengan adanya cadangan yang terpisah, organisasi dapat dengan mudah memulihkan data mereka tanpa harus memenuhi permintaan tebusan. Backup data juga dapat dilakukan melalui cloud atau perangkat penyimpanan fisik yang terisolasi dari jaringan utama, memastikan bahwa data tetap dapat dipulihkan meskipun terjadi serangan ransomware yang parah.(Yusnanto et al., 2019)

Namun, meskipun teknologi menawarkan banyak solusi dalam pencegahan ransomware, teknologi ini tidak sempurna. Ransomware yang semakin canggih dapat menembus lapisan pertahanan ini, misalnya dengan teknik enkripsi yang lebih kuat atau penyebaran melalui celah keamanan yang belum ditemukan. Oleh karena itu, teknologi harus diterapkan dalam kombinasi dengan kebijakan yang komprehensif dan pemantauan yang berkelanjutan.

3. Integrasi Edukasi Pengguna dan Teknologi dalam Mencegah Ransomware

Meskipun baik edukasi pengguna maupun teknologi memiliki peran yang sangat penting dalam pencegahan ransomware, hasil yang optimal hanya dapat tercapai jika keduanya diintegrasikan dengan baik. Edukasi pengguna memberikan dasar yang kuat dalam meningkatkan kesadaran dan pemahaman tentang ancaman, sementara teknologi berfungsi untuk memberikan perlindungan proaktif yang dapat mendeteksi dan mengatasi serangan secara otomatis. Beberapa penelitian menunjukkan bahwa kombinasi keduanya lebih efektif daripada mengandalkan satu pendekatan saja. Sebagai contoh, penelitian yang dilakukan oleh Symantec (2020) menunjukkan bahwa organisasi yang menggabungkan pelatihan pengguna secara rutin dengan penerapan teknologi keamanan yang canggih memiliki tingkat keberhasilan yang lebih tinggi dalam mencegah serangan ransomware. Dengan edukasi yang memadai, pengguna dapat lebih berhati-hati dalam menggunakan perangkat mereka dan mengenali potensi ancaman, sementara teknologi dapat bertindak sebagai lapisan tambahan untuk mendeteksi serangan yang tidak terdeteksi oleh pengguna.(Broadcom, 2020)

Selain itu, penting untuk mengembangkan kebijakan yang mendukung penerapan kedua pendekatan ini. Kebijakan yang mengutamakan pelatihan berkelanjutan, pengawasan terhadap aktivitas pengguna, serta implementasi teknologi yang tepat akan menciptakan lingkungan yang lebih aman dari ancaman ransomware. Organisasi juga perlu memastikan bahwa seluruh karyawan, dari level bawah hingga atas, terlibat dalam menjaga keamanan informasi dan data perusahaan.

4. Tantangan dalam Implementasi Pencegahan Ransomware

Meskipun pencegahan ransomware berbasis edukasi pengguna dan teknologi memiliki potensi yang besar, implementasinya tidak tanpa tantangan. Salah satu tantangan terbesar adalah resistensi dari pengguna terhadap perubahan. Banyak pengguna yang menganggap pelatihan atau kebijakan keamanan sebagai beban tambahan yang tidak penting, sehingga mereka cenderung mengabaikan atau tidak mengikuti instruksi yang diberikan. Di sisi teknologi, tantangan yang lebih teknis juga muncul, terutama terkait dengan kecepatan perkembangan ransomware yang semakin canggih. Teknologi yang digunakan untuk mendeteksi dan mencegah serangan harus terus diperbarui dan ditingkatkan agar dapat mengikuti perkembangan ancaman baru yang muncul. Selain itu, penggunaan teknologi yang sangat canggih bisa menambah biaya bagi organisasi, terutama untuk usaha kecil dan menengah yang memiliki anggaran terbatas untuk investasi di bidang keamanan siber.(Sadikin, 2023)

5. Rekomendasi untuk Penguatan Pencegahan Ransomware

Berdasarkan pembahasan di atas, beberapa rekomendasi yang dapat diperhatikan untuk memperkuat pencegahan ransomware melalui peningkatan Program Edukasi Organisasi harus mengimplementasikan pelatihan yang bersifat praktis dan berkelanjutan, yang mencakup simulasi serangan phishing, pengenalan terhadap perilaku berisiko, serta peningkatan kesadaran tentang pentingnya menjaga keamanan data. Investasi dalam Teknologi Keamanan, organisasi perlu mengadopsi teknologi keamanan yang canggih, seperti sistem deteksi intrusi berbasis AI, firewall yang lebih kuat, serta enkripsi data dan pencadangan secara berkala. Kebijakan Keamanan yang Komprehensif, melalui pengembangan kebijakan internal yang mengutamakan keamanan data, melibatkan seluruh level organisasi dalam menjaga keamanan siber, serta memastikan bahwa teknologi dan pelatihan yang tepat diterapkan secara konsisten.(Anasrullah, 2024)

Hasil penelitian ini selaras dengan temuan yang dirilis oleh Kaspersky (2019) menunjukkan bahwa program edukasi pengguna memiliki pengaruh signifikan dalam mengurangi risiko serangan ransomware. Dalam studi ini, Kaspersky mengidentifikasi bahwa organisasi yang rutin melakukan pelatihan mengenai ancaman ransomware, terutama melalui simulasi phishing dan pembelajaran tentang tanda-tanda potensi serangan, mengalami penurunan insiden ransomware hingga 30% dalam kurun waktu satu tahun. Pengguna yang mengikuti pelatihan ini cenderung lebih waspada dan menghindari tindakan berisiko, seperti mengklik email yang mencurigakan atau mengunduh lampiran berbahaya. Temuan ini mendukung konsep bahwa pemberdayaan pengguna dengan pengetahuan dasar tentang ancaman keamanan siber, terutama ransomware, dapat mengurangi jumlah serangan yang terjadi. Namun, penelitian ini juga mencatat bahwa efektivitas pelatihan sangat bergantung pada kontinuitas dan keterlibatan seluruh karyawan dalam program tersebut.(Community, 2019)

Dalam sebuah penelitian yang dipublikasikan oleh Symantec (2020), ditemukan bahwa penggunaan perangkat lunak keamanan, seperti antivirus dan perangkat pemantauan lalu lintas jaringan (IDS/IPS), mampu menurunkan tingkat infeksi ransomware hingga 40% di perusahaan yang mengimplementasikannya dengan benar. Penelitian ini juga menunjukkan bahwa teknologi enkripsi data dan cadangan data secara berkala sangat membantu dalam mitigasi kerugian finansial akibat serangan ransomware. (Broadcom, 2020) Enkripsi memastikan bahwa meskipun data dienkripsi oleh ransomware, data tetap aman dan tidak dapat diakses tanpa kunci dekripsi yang sah. Selain itu, temuan ini juga mengungkapkan bahwa teknologi yang lebih canggih, seperti sistem berbasis kecerdasan buatan (AI) untuk mendeteksi anomali, dapat menanggulangi ancaman ransomware yang semakin kompleks. Namun, penelitian ini menyoroti tantangan dalam implementasi, terutama terkait dengan biaya yang diperlukan untuk investasi dalam teknologi tinggi, serta kebutuhan akan pemeliharaan dan pembaruan sistem yang terus-menerus.(Nadwan et al., 2024)

Sebuah studi yang diterbitkan oleh Journal of Cybersecurity Education, Research and Practice (2021) meneliti efektivitas penggabungan edukasi pengguna dengan penerapan teknologi keamanan dalam organisasi. Hasil penelitian menunjukkan bahwa kombinasi keduanya menghasilkan pengurangan yang lebih besar dalam jumlah serangan ransomware dibandingkan dengan pendekatan tunggal. Organisasi yang menggabungkan pelatihan pengguna tentang kesadaran keamanan dengan perangkat lunak deteksi malware dan strategi cadangan data melaporkan penurunan insiden serangan ransomware hingga 50%. Penelitian ini juga mencatat bahwa pelatihan yang disesuaikan dengan level pemahaman teknis pengguna dan teknologi yang sesuai dengan kebutuhan organisasi masing-masing sangat penting untuk keberhasilan pencegahan ransomware. Pengguna yang dilatih untuk mengenali teknik serangan seperti phishing dan social engineering menjadi lebih waspada terhadap upaya peretasan, sementara teknologi membantu mencegah ancaman yang tidak dapat dideteksi oleh manusia.(Ravichandran et al., 2025)

Penelitian oleh Hackbarth & George (2020) mengungkapkan tantangan utama dalam mengedukasi pengguna untuk mencegah ransomware. Mereka menemukan bahwa meskipun banyak organisasi yang telah meluncurkan pelatihan keamanan siber untuk karyawan mereka, masih terdapat kesenjangan dalam pemahaman dan penerapan pengetahuan yang diberikan. Salah satu temuan kunci adalah ketidakpedulian atau keengganan pengguna untuk mengikuti pelatihan yang dianggap kurang relevan dengan tugas sehari-hari mereka. Faktor lain yang memengaruhi efektivitas pelatihan adalah kebosanan terhadap konten yang terlalu teknis atau tidak dapat dipahami oleh pengguna dengan sedikit latar belakang teknis. Penelitian ini menyarankan pendekatan pelatihan yang lebih menarik dan relevan, seperti menggunakan skenario dunia nyata yang dapat diaplikasikan oleh

pengguna sehari-hari. Selain itu, pentingnya pengawasan dan evaluasi berkelanjutan terhadap pelatihan menjadi sangat jelas dalam penelitian ini untuk memastikan bahwa pelatihan yang diberikan benar-benar memberikan dampak yang signifikan terhadap kesadaran dan perilaku pengguna.(Hackbarth et al., 2012)

Penelitian oleh Zhao et al. (2021) mengeksplorasi faktor-faktor yang mempengaruhi keberhasilan serangan ransomware pada infrastruktur teknologi informasi (TI) organisasi. Mereka menemukan bahwa kelemahan dalam kebijakan keamanan dan pengelolaan perangkat lunak yang tidak terbarui merupakan dua penyebab utama yang memungkinkan ransomware berhasil menyusup ke sistem organisasi. Dalam penelitian ini, ditemukan bahwa organisasi yang mengadopsi kebijakan keamanan berbasis pembaruan sistem yang rutin dan pengelolaan patch perangkat lunak yang baik cenderung memiliki tingkat serangan ransomware yang lebih rendah. Penelitian ini menekankan pentingnya pengelolaan perangkat lunak yang terpusat dan pembaruan perangkat lunak secara otomatis untuk meminimalisir celah yang dapat dimanfaatkan oleh pelaku kejahatan siber. Temuan ini memberikan wawasan penting bagi organisasi dalam merancang strategi pencegahan yang mencakup pembaruan perangkat lunak dan pengelolaan patch sebagai langkah preventif terhadap ransomware.(Zhao et al., 2021)

Penelitian oleh Chavez et al. (2020) membahas pengaruh penggunaan mata uang kripto, seperti Bitcoin, dalam transaksi pembayaran tebusan pada serangan ransomware. Ditemukan bahwa penggunaan mata uang kripto memudahkan pelaku kejahatan untuk menerima pembayaran secara anonim, sehingga meningkatkan insentif untuk melancarkan serangan ransomware. Penelitian ini juga menunjukkan bahwa meskipun beberapa negara telah mencoba melarang atau mengatur penggunaan mata uang kripto, adopsi global yang semakin meningkat membuatnya tetap menjadi metode utama bagi pelaku kejahatan dalam menuntut tebusan.(Chávez et al., 2020)

## KESIMPULAN

Ransomware merupakan ancaman serius dalam dunia digital yang tidak hanya menimbulkan kerugian finansial, tetapi juga mengancam kelangsungan operasional organisasi dan integritas data pengguna. Berdasarkan hasil studi kepustakaan, dapat disimpulkan bahwa upaya pencegahan ransomware memerlukan pendekatan yang komprehensif dan terintegrasi. Edukasi pengguna menjadi fondasi utama dalam membentuk kesadaran dan kebiasaan aman dalam berinteraksi dengan sistem informasi. Penggunaan teknologi keamanan seperti firewall, antivirus, sistem deteksi intrusi, serta pencadangan data secara berkala juga terbukti efektif dalam meminimalkan dampak serangan. Literasi digital yang kuat, dibarengi dengan kebijakan keamanan yang jelas dan implementasi teknologi mutakhir, dapat meningkatkan ketahanan siber suatu organisasi. Dengan demikian, kombinasi antara pendekatan edukatif dan teknologis merupakan strategi preventif yang paling efektif dalam menghadapi ancaman ransomware di era digital saat ini..

## DAFTAR PUSTAKA


Anasrullah, F. (2024). Pencegahan Ransomware Pada Server on Premise Menggunakan Teknik Security Hardening. *Jurnal Informatika Dan Teknik Elektro Terapan*, *12*(3). https://doi.org/10.23960/jitet.v12i3.5105

Broadcom. (2020). *We stop threats hiding in plain sight. Endpoint, Network, Email, Cloud. However they attack, we've got you covered.* https://sep.securitycloud.symantec.com/v2/landing

Brunnstein, K. (1999). From AntiVirus to AntiMalware Software and Beyond: Another Approach to the Protection of Customers from Dysfunctional System Behaviour. *National Information Systems Security Conference*.

Chávez, M. N., Morales, R. A., López-Crisosto, C., Roa, J. C., Allende, M. L., & Lavandero, S. (2020). Autophagy Activation in Zebrafish Heart Regeneration. *Scientific Reports*, *10*(1), 1–11. https://doi.org/10.1038/s41598-020-59106-z

Community, I. (2019). *Kaspersky Support Forum*. https://forum.kaspersky.com/

Ferdiansyah. (2018). Analisis Aktivitas Dan Pola Jaringan Terhadap Eternal Blue Dan Wannacry Ransomware. *JUSIFO (Jurnal Sistem Informasi)*, *2*(1), 44–59. http://eprints.binadarma.ac.id/3873/1/Ferdiansyah-Analisis Aktivitas dan Pola Jaringan Terhadap Eternal Blue dan Wannacry Ransomware.pdf

Hackbarth, M., Pavkov, T., Wetchler, J., & Flannery, M. (2012). Natural Disasters: An Assessment of Family Resiliency Following Hurricane Katrina. *Journal of Marital and Family Therapy*, *38*(2), 340–351. https://doi.org/10.1111/j.1752-0606.2011.00227.x

Hartono, B. (2023). Ransomware: Memahami Ancaman Keamanan Digital. *Bincang Sains Dan Teknologi*, *2*(02), 55–62. https://doi.org/10.56741/bst.v2i02.353

Kristalia, B. Y. Y., & Wibisono, I. W. (2024). Ancaman Siber Dan Penguatan Kedaulatan Digital Indonesia Dari Perspektif Geopolitik Digital. *Jurnal Ilmiah Multidisiplin*, *3*(02), 83–93. https://doi.org/10.56127/jukim.v3i02.1584

Nadwan, H., Putri, M. A., & Akbar, M. R. (2024). Penggunaan AI Sebagai Media Melakukan Tindak Pidana Malware Dikaitkan Dengan Teori Progressivesme Menurut Johann Heinrich Pestalozzi Dalam Peraturan …. *Das Sollen: Jurnal Kajian …*, *2023*, 1–17. https://doi.org/10.11111/dassollen.xxxxxxx

Ravichandran, R., Singh, S., & Sasikala, P. (2025). *Exploring School Teachers ' Cyber Security Awareness ,*

*Experiences , and Practices in the Digital Age Exploring School Teachers ' Cyber Security Awareness , Experiences , and*. *2025*(1).
Sadikin, N. (2023). Implementasi Security control pada Infrastruktur Teknologi Informasi untuk Mencegah dan Menanggulangi Malware Ransomware untuk Keamanan Informasi Perusahaan. *Jurnal Maklumatika*, *10*(2), 77–86. https://maklumatika.i-tech.ac.id/index.php/maklumatika/article/view/234
Susanto, E., Antira, Lady, Kevin, K., Stanzah, E., & Majid, A. A. (2023). Manajemen Keamanan Cyber Di Era Digital. *Journal of Business And Entrepreneurship*, *11*(1), 23. https://doi.org/10.46273/jobe.v11i1.365
Wijanarko, R. P., Moch Rezeki Setiawan, Siti Mukaromah, & Abdul Rezha Efrat Najaf. (2023). Analisis Dan Simulasi Serangan Ransomware Terhadap Database Bank Syariah Indonesia. *Prosiding Seminar Nasional Teknologi Dan Sistem Informasi*, *3*(1), 106–115. https://doi.org/10.33005/sitasi.v3i1.436
Yusnanto, T., Machmudi, A., Mustofa, K., Manajemen, ), Stmik, I., & Patria, B. (2019). Pengaruh Kerusakan Perangkat Penyimpanan Hardisk Dan Flashdisk Terhadap Virus Kaspersky Internet Security. *Jurnal TRANSFORMASI*, *15*(2), 177–185.
Zhao, S., Chancellor, W., Jackson, T., & Boult, C. (2021). *Productivity as a measure of performance: ABARES perspective*. *September*.