E-ISSN : 3025-1311
https://ejournal.warunayama.org/kohesi

Kohesi: Jurnal Multidisiplin Saintek
Volume 3 No 9 Tahun 2024

ANALISIS KEAMANAN SISTEM KOMPUTER PADA ORGANISASI ARSITERTUR KOMPUTER

Mochamad Yogi Febriansyah[1], Muhammad Azhar Firdaus[2], Haeva Salsabila[3], Daffa Wahid Sya'bani[4], Noval Fathur Rahman[5]

Program Studi Informatika, Fakultas Sains, UIN Sultan Maulana Hasanudin Banten, Indonesia
Email: [1]yogif534@gmail.com, [2] azharxbd@gmail.com, [3] haevasalsabila333@gmail.com, [4]wahiddaffa332@gmail.com, [5] novalfathurrahman2@gmail.com,

Abstrak

In the era of rapid technological advancement, the general public extensively uses devices such as computers and smartphones, leading to increased awareness of data security. One method to protect computers is by installing anti-virus applications. These anti-virus programs help prevent malicious software from infiltrating our computers, although their usage may not always be entirely comfortable
***Keywords**: Devices, Anti virus, Cyber Issues.*

Abstrak

Di era perkembangan teknologi yang pesat, masyarakat luas menggunakan perangkat seperti komputer dan smartphone, sehingga pada umumnya mereka menjadi lebih sadar akan pentingnya keamanan data. Salah satu metode untuk melindungi komputer adalah dengan menginstal aplikasi anti-virus. Dengan program anti-virus ini, setidaknya kita dapat mencegah masuknya perangkat lunak berbahaya ke dalam komputer, meskipun penggunaan anti-virus tersebut mungkin tidak selalu nyaman.
Kata kunci: Perangkat, Anti virus, Masalah Cyber

PENDAHULUAN

Perkembangan teknologi, terutama dalam bidang keamanan komputer, menjadi hal yang sangat penting. Namun, sering kali pemilik dan pengelola sistem informasi kurang memberikan perhatian yang memadai terhadap masalah keamanan. Keamanan kerap kali hanya menjadi prioritas kedua atau bahkan terakhir dalam daftar aspek yang dianggap penting. Apabila keamanan menghambat kinerja sistem, sering kali elemen keamanan ini dikurangi atau bahkan dihilangkan (Wirdasari, 2008).

Fungsi utama keamanan komputer adalah melindungi informasi dari pencurian data. Untuk mencegah data kita dicuri oleh pihak yang tidak bertanggung jawab, pentingnya keamanan bagi perlindungan informasi kita (Ramadhani, 2017). Di era digital ini, serangan siber memiliki dampak besar bagi berbagai instansi, baik negeri maupun swasta. Jika tidak ditangani dengan baik, semua pihak akan dirugikan. Oleh karena itu, pembuatan keamanan server, penguncian data, serta pembuatan duplikat data harus diperhatikan secara berkala dan mendetail agar lingkungan yang telah dibuat berjalan sesuai harapan dan tidak terjadi hal-hal yang tidak diinginkan di kemudian hari. Maka dari itu, pentingnya keamanan komputer sangat ditekankan dalam era serba baru ini.

Saat ini, banyak orang berusaha membangun sistem guna mengamankan informasi mereka dari serangan virus atau penipuan oleh pihak lain. Perkembangan teknologi keamanan komputer menjadi kunci utama dan banyak dibicarakan. Terselip potensi bisnis di balik teknologi keamanan komputer, di mana para pengembang yang memiliki

kemampuan dalam menciptakan sistem perlindungan data dari serangan virus atau pihak yang tidak diinginkan dapat memanfaatkan peluang ini.

Keamanan tidak seharusnya menghalangi atau menyulitkan proses transaksi dan pengambilan keputusan. Ada berbagai metode yang dapat digunakan untuk melindungi data dan informasi dalam suatu sistem. Perlindungan data dibagi menjadi dua jenis: preventif dan kuratif. Langkah preventif bertujuan untuk memastikan data tetap aman dari kerusakan, kehilangan, atau pencurian. Sementara itu, langkah kuratif dilakukan ketika data sudah terinfeksi virus, sistem terkena worm, atau ada eksploitasi terhadap celah keamanan.

Dalam makalah ini, akan dibahas mengenai identifikasi dan analisis berbagai kerentanan sistem komputer, langkah-langkah yang dapat diambil untuk mengatasi kerentanan tersebut, praktik terbaik dalam keamanan sistem komputer, serta evaluasi penggunaan antivirus yang sesuai dengan kebutuhan organisasi.

METODOLOGI PENELITIAN

Penelitian ini menggunakan metode Analisis pustaka. Pendekatan ini mencakup pencarian dan analisis mendalam terhadap berbagai sumber tertulis yang sesuai, berupa artikel, jurnal, dan informasi lainnya yang berhubungan dengan topik yang diteliti. Informasi yang diperoleh dari analisis pustaka ini kemudian digunakan sebagai referensi untuk mendukung penelitian. Hasil dari kajian literatur tersebut akan digunakan untuk menelaah dan mendiskusikan analisis keamanan sistem komputer dalam konteks organisasi arsitektur komputer.

HASIL DAN PEMBAHASAN

Ada berbagai macam penelitian terkait masalah keamanan pada komputer

1) Penilaian Kerentanan: Penilaian kerentanan ialah proses mengidentifikasi dan mengevaluasi potensi kerentanan dalam sistem komputer Penilaian kerentanan dapat dilakukan secara manual atau menggunakan alat pemindaian kerentanan.
2) Tes Penetrasi: Tes penetrasi adalah simulasi serangan terhadap sistem komputer untuk menguji efektivitas kontrol keamanan.Tes penetrasi dapat dilakukan oleh tim internal atau perusahaan keamanan
3) Analisis Keamanan Jaringan: Analisis keamanan jaringan adalah proses menganalisis lalu lintas jaringan untuk mencari aktivitas mencurigakan. Analisis keamanan jaringan dapat dilakukan menggunakan alat analisis jaringan.

1. Metodologi Analisis Keamanan Sistem Komputer

Berikut beberapa metodologi analisis keamanan sistem komputer yang berbeda, tetapi umumnya metodologi tersebut mengikuti langkah-langkah berikut:

1) Penentuan Lingkup: Langkah pertama adalah menentukan lingkup analisis, yaitu sistem komputer mana yang akan dianalisis.
2) Pengumpulan Data: Langkah selanjutnya adalah mengumpulkan data tentang sistem komputer, termasuk perangkat keras, perangkat lunak, jaringan, dan konfigurasi sistem.
3) Identifikasi Kerentanan: Data yang dikumpulkan kemudian dianalisis untuk mengidentifikasi potensi kerentanan dalam sistem komputer. Kerentanan dapat berupa kelemahan dalam perangkat lunak, konfigurasi sistem yang tidak aman, atau praktik keamanan yang tidak memadai.
4) Evaluasi Kerentanan: Kerentanan yang diidentifikasi kemudian dievaluasi untuk menentukan tingkat keparahannya. Tingkat keparahan kerentanan dihitung berdasarkan

faktor-faktor seperti kemungkinan dieksploitasi, dampak potensial jika dieksploitasi, dan kemudahan eksploitasi.

5) Rekomendasi Perbaikan: Berdasarkan hasil evaluasi kerentanan, rekomendasi perbaikan kemudian dikembangkan untuk mengatasi kerentanan tersebut. Rekomendasi perbaikan dapat berupa menerapkan patch perangkat lunak, mengubah konfigurasi sistem, atau menerapkan praktik keamanan yang lebih baik.
6) Dokumentasi: Hasil analisis keamanan sistem komputer kemudian didokumentasikan dalam laporan yang komprehensif. Laporan tersebut harus mencakup temuan analisis, rekomendasi perbaikan, dan rencana tindak lanjut.

2. Alat Analisis Keamanan Sistem Komputer

Ada berbagai alat yang tersedia untuk membantu analisis keamanan sistem komputer. Alat-alat ini dapat dikategorikan menjadi beberapa jenis, seperti:

1) Alat Pemindaian Kerentanan: Alat pemindaian kerentanan digunakan untuk secara otomatis memindai sistem komputer untuk mencari potensi kerentanan.
2) Alat Analisis Keamanan Jaringan: Alat analisis keamanan jaringan digunakan untuk menganalisis lalu lintas jaringan untuk mencari aktivitas mencurigakan.
3) Alat Penilaian Keamanan Host: Alat penilaian keamanan host digunakan untuk menilai keamanan sistem komputer individual.
4) Alat Tes Penetrasi: Alat tes penetrasi digunakan untuk mensimulasikan serangan terhadap sistem komputer untuk menguji efektivitas kontrol keamanan.

3. Tantangan Analisis Keamanan Sistem Komputer

Ada beberapa tantangan yang dihadapi dalam analisis keamanan sistem komputer, seperti:

1) Kompleksitas Sistem Komputer: Sistem komputer menjadi semakin kompleks, dengan berbagai perangkat keras, perangkat lunak, dan jaringan yang saling terhubung. Hal ini membuat analisis keamanan sistem komputer menjadi lebih sulit dan memakan waktu.
2) Ketersediaan Alat: Tidak semua alat analisis keamanan sistem komputer tersedia secara gratis atau dengan biaya yang terjangkau. Hal ini dapat membatasi kemampuan organisasi arsitektur komputer untuk melakukan analisis keamanan sistem komputer secara menyeluruh.
3) Kurangnya Keahlian: Diperlukan keahlian khusus untuk melakukan analisis keamanan sistem komputer. Hal ini dapat membuat sulit bagi organisasi arsitektur komputer untuk menemukan personel yang memenuhi syarat untuk melakukan analisis tersebut.

4. Praktik Terbaik Analisis Keamanan Sistem Komputer

Berikut adalah beberapa praktik terbaik untuk analisis keamanan sistem komputer:

1) Melakukan analisis keamanan sistem komputer secara teratur: Analisis keamanan sistem komputer harus dilakukan secara teratur untuk mengidentifikasi dan mengatasi potensi kerentanan baru.
2) Melibatkan berbagai pihak: Analisis keamanan sistem komputer harus melibatkan berbagai pihak, seperti staf IT, manajemen, dan pengguna akhir.
3) Menggunakan alat yang tepat

Virus komputer adalah sebuah program yang memiliki kemampuan untuk menggandakan dirinya dengan menyalin ke dalam program atau dokumen lainnya. Virus komputer ini dapat diibaratkan seperti virus biologis yang menginfeksi sel dalam

organisme hidup. Virus komputer dapat menyebabkan kerusakan pada perangkat keras komputer dengan menjalankan program tertentu di komputer, merusak data pada dokumen, mengganggu pengguna, atau bahkan tidak menunjukkan efek apapun. Efek dari virus komputer sangat bervariasi, mulai dari merusak data pada dokumen, mengganggu pengguna, hingga tidak menimbulkan efek apapun (Susilo, 2003).

Oleh karena itu, disarankan untuk menginstal antivirus setelah memasang sistem operasi (OS). Beberapa hal yang perlu diperhatikan dalam memilih antivirus antara lain:

1. Rate Detection Test

Pengujian ini melibatkan penggunaan basis data tanda tangan. Antivirus diuji terhadap banyaknya sampel virus, dengan tujuan menentukan antivirus mana yang memiliki tingkat deteksi tertinggi terhadap sampel tersebut.

2. Heuristic/Prospective/Generic Test

Pengujian ini melibatkan pendeteksian virus/malware baru yang belum terdaftar dalam basis data tanda tangan dengan menggunakan basis data tanda tersebut sebagai acuan. Jika ada ciri-ciri virus/malware yang terdeteksi, fungsi heuristik akan mendeteksinya.

3. Performance Test

Menggunakan perangkat lunak antivirus tentu akan mengonsumsi sumber daya komputer, seperti CPU dan memori. Oleh karena itu, sangat penting untuk memilih produk antivirus yang memiliki manajemen sumber daya yang efisien sehingga tidak mengurangi kinerja komputer. Beberapa Macam Antivirus:

1) Avast Antivirus:
Sistem operasi memang sudah memiliki perlindungan, tetapi itu belum cukup.. Dengan menginstal perangkat lunak ini, pengguna dapat mengaktifkan pemindaian cerdas otomatis dengan memeriksa perangkat lunak, file, dan aplikasi untuk menemukan kerentanan yang bisa dieksploitasi oleh malware. Avast juga mampu mengirim file yang dianggap mencurigakan ke cloud untuk analisis lebih lanjut, memberikan peringatan tentang ancaman yang terdeteksi, serta menawarkan berbagai fitur tambahan lainnya.

1) Keamanan jaringan Wi-Fi: Terhubung ke jaringan Wi-Fi dengan lebih aman dan mencegah penjahat siber serta penyusup jahat mengakses jaringan, sehingga file sensitif dan pribadi tetap terlindungi dari mereka.
2) Menjelajah internet dan berkirim email dengan lebih amanTetap lebih aman saat menjelajah internet, berkirim email, atau bekerja secara online. Membantu dalam memblokir situs web berbahaya dan unduhan tidak aman, serta membantu mencegah perangkat Anda agar tidak dibajak dan dijadikan bagian dari botnet.
3) Menjelajah internet dan berkirim email dengan lebih aman. Tingkatkan keamanan saat menjelajah internet, mengirim email, atau bekerja online. Membantu memblokir situs web berbahaya dan unduhan yang tidak aman, serta mencegah perangkat dari pembajakan dan dijadikan bagian dari botnet.
4) Perlindungan ransomware. untuk mengubah, membekukan, atau mengunci file-file pribadi dengan tujuan tertentu.

Gambar 1

2) Bitdefender Antivirus

Dikenal sebagai antivirus yang ringan dan memiliki perlindungan yang sangat baik.

a) Memberikan Informasi Tanpa Gangguan

Tidak seperti produk keamanan lainnya yang terus-menerus mengganggu dengan permintaan izin, Bitdefender dengan lembut memberikan informasi tentang ancaman, kemudian segera menyingkir.

b) Pemindaian Harian Tanpa Membuat Pengguna Terganggu

Kekhawatiran mengenai pemindaian yang sangat lambat dan membuat sistem menjadi terhenti tidak perlu ada. Pemindaian Bitdefender yang efisien menangkap setiap ancaman tanpa mengganggu kinerja.

c) Tidak Membebani atau Mengganggu Aplikasi Lain

Beberapa alat keamanan sangat mengganggu hingga terasa seperti virus. Fitur-fitur Bitdefender tetap terkandung dalam satu aplikasi, sehingga tidak terlihat hingga pengguna ingin melihatnya.

Gambar 2

3) Kaspersky AntivirusMerek mapan dengan reputasi keamanan siber yang kuat, menawarkan perlindungan komprehensif terhadap berbagai ancaman.

a) Perlindungan Komprehensif

Menghentikan Semua Ancaman dari Malware hingga RansomwareBitdefender memblokir segala bentuk ancaman, mulai dari malware dan virus hingga ransomware dan aplikasi mata-mata, memastikan Anda selalu dilindungi sepenuhnya.

b) Pengawasan Komprehensif

Memelihara Privasi Kata Sandi, Konten, dan AktivitasDengan VPN, Kaspersky Password Manager, dan solusi kami lainnya, privasi kata sandi, konten, dan aktivitas Anda akan terjaga dengan baik.

c) Kinerja Optimal

Lancar Tanpa Gangguan saat Berbelanja Online atau Bermain Game.Nikmati pengalaman berbelanja online dan bermain game tanpa gangguan, karena komputer Anda tetap berjalan lancar tanpa hambatan.

Gambar 3

4) McAfee Antivirus: Merek antivirus klasik yang menawarkan perlindungan dasar hingga paket keamanan internet lengkap mencakup

a) Perlindungan web McAfee WebAdvisor
Memungkinkan menghindari serangan sebelum terjadi dengan peringatan yang jelas tentang situs web, tautan, dan file berisiko, sehingga dapat menjelajah, berbelanja, dan melakukan transaksi perbankan dengan percaya diri.

b) Fitur Pengoptimalan PC
Membantu PC bekerja lebih cepat sekaligus memastikan memiliki keamanan terbaik. Web Boost membantu menyelamatkan baterai dan bandwidth dari gangguan pemutaran video otomatis dengan menjedanya secara otomatis. Dan dengan App Boost, aplikasi yang sedang dikerjakan secara aktif akan otomatis menerima peningkatan sumber daya, sehingga pekerjaan dapat diselesaikan lebih cepat.

c) Dengan McAfee Total Protection untuk 10 perangkat, juga mendapatkan akses ke McAfee Safe Family
Yang memberikan kontrol orang tua yang kuat untuk PC Windows dan perangkat Android/iOS anak. Dilengkapi dengan berbagai fitur berguna, Safe Family memberi serangkaian alat ekstra untuk mengatur kehidupan digital anak-anak, mulai dari membantu membangun kebiasaan baik hingga mengelola penggunaan aplikasi dan waktu online mereka. Bahkan dapat melacak lokasi saat sedang beraktivitas di luar ruangan.

Gambar 4

5) Norton 360 Antivirus
Paket keamanan internet yang menawarkan perlindungan menyeluruh, termasuk antivirus, firewall, perlindungan pencurian identitas, dan lainnya.

Memilih Antivirus Terbaik:

Saat memilih antivirus, pertimbangkan faktor-faktor berikut:

1) Kebutuhan Anda: Apakah Anda hanya membutuhkan perlindungan dasar dari virus, atau memerlukan perlindungan yang lebih komprehensif seperti firewall dan perlindungan pencurian identitas?
2) Perangkat yang digunakan: Apakah Anda membutuhkan antivirus untuk Windows, macOS, Android, atau iOS?
3) Harga: Beberapa antivirus gratis, sementara yang lain memerlukan langganan berbayar.
4) Performa: Pilih antivirus yang tidak terlalu membebani sumber daya komputer Anda.
5) Ulasan pengguna: Baca ulasan pengguna untuk mengetahui pengalaman orang lain dengan antivirus tersebut.

Selain antivirus, penting juga untuk menerapkan praktik keamanan siber yang baik, seperti:

1) Menjaga agar perangkat lunak tetap terbaru.
2) Pastikan untuk menggunakan kombinasi kata sandi yang sulit ditebak dan berbeda untuk setiap akun yang Anda miliki.
3) Selalu pertimbangkan dengan hati-hati sebelum mengklik tautan atau membuka lampiran dari email yang tidak Anda kenal, karena bisa jadi mengandung potensi ancaman keamanan..
4) Mencadangkan data Anda secara teratur.

KESIMPULAN

Analisis keamanan sistem komputer melibatkan evaluasi menyeluruh terhadap potensi ancaman dan kerentanan yang mungkin timbul pada sistem komputer suatu organisasi. Langkah-langkah penting dalam analisis ini mencakup mengidentifikasi potensi ancaman, mengevaluasi kerentanan sistem, menilai risiko, dan menerapkan praktik terbaik untuk mengurangi risiko serangan.

Praktik terbaik dalam hal ini termasuk penggunaan teknologi keamanan seperti firewall, antivirus, dan enkripsi data, serta menerapkan kebijakan keamanan yang ketat seperti manajemen akses yang tepat dan pelatihan keamanan untuk pengguna. Monitoring terus-menerus terhadap sistem juga penting untuk mendeteksi aktivitas mencurigakan atau ancaman potensial.

Dengan menerapkan praktik terbaik tersebut, sebuah organisasi dapat meningkatkan keamanan sistem komputer mereka, mengurangi risiko serangan, dan menjaga keamanan siber yang solid. Hal ini esensial untuk melindungi data sensitif, menjaga kontinuitas operasional organisasi, dan mempertahankan kepercayaan pelanggan.

REFERENCES

D3 Teknik Komputer A.Md.Kom. "Mengenal Vulnerability Assessment: Langkah Penting dalam Keamanan Sistem Informasi." stekom.ac.id.

IAS. "Penilaian Kerentanan dan Pengujian Penetrasi." ias-indonesia.org.

ITEBA. "5 Antivirus Terbaik untuk Windows dan MacOS." ITEBA Blog.

Maya Safitri, E., Sefri Larasati, A., & Rizki Hari, S. (2020*). Analisis Keamanan Sistem Informasi E-Banking Di Era Industri 4.0: Studi Literatur. Jurnal Ilmiah Teknologi Informasi Dan Robotika,* 2(1).

Zulfariana, Z., Zhafar, E. N., & Mikdar, M. (2011). *Analisa Algoritma Sistem Keamanan Komputer Menggunakan Sidik Jari dengan Metode Poin Minutiae pada HP Compaq 2210B Notebook PC.*

Afrian, F. (2019). *Pentingnya Keamanan Komputer dan Teknik Pengamanan Komputer.* Riau, 6.

Setiawan, E. (2021). *Keamanan Sistem Informasi*,, 1(1), 1-10.