Contents lists available at MID Publisher International

Technology Sciences Insights Journal

Journal homepage: https://journal.midpublisher.com/index.php/tsij

Mitigasi Malware dan Ransomeware Pada Jaringan Komputer

Rakhmadi Rahman, Andi Putri Wildana*

Prodi Sistem Informasi, Fakultas Sains, Institut Teknologi Bacharuddin Jusuf Habibie, Parepare, Indonesia

INFORMASI ARTIKEL

Sejarah Artikel:
Diterima Juni 2024
Revisi Juni 2024
Diterima Juli 2024

Kata Kunci:
Malware, Ransomware, Keamanan Network, Pencegahan, Manajemen Patch, Detection and Response Endpoint (EDR), Deep Packet Inspection (DPI)

*Penulis Korespondensi:
andiputriwildana@gmail.com

ABSTRAK

Keamanan jaringan komputer menghadapi tantangan signifikan dari ancaman malware dan ransomware yang semakin canggih. Laporan ini membahas jenis-jenis malware dan ransomware yang paling umum dan berbahaya, metode deteksi yang efektif, serta strategi mitigasi yang dapat diterapkan untuk mencegah dan merespons serangan. Penelitian ini menggunakan studi literatur untuk mengidentifikasi pendekatan terbaik dalam mendeteksi dan mengatasi ancaman siber ini. Hasilnya menunjukkan pentingnya penerapan solusi keamanan terintegrasi, edukasi pengguna, dan inovasi teknologi dalam menjaga keamanan jaringan komputer

ABSTRACT

Computer network security faces significant challenges from increasingly sophisticated malware and ransomware threats. This report discusses the most common and dangerous types of malware and ransomware, as well as effective detection methods and mitigation strategies that can be implemented to prevent and respond to attacks. This research uses literature studies to identify the best approach to detecting and overcoming this cyber threat. The results show the importance of implementing integrated security solutions, user education, and technological innovation in maintaining computer network security.

PENDAHULUAN

Serangan siber sekarang menjadi ancaman besar bagi jaringan komputer di berbagai industri di era komputer. Dua jenis serangan yang paling berbahaya dan umum adalah ransomware dan malware. Malware memiliki kemampuan untuk mencuri data sensitif, menyebabkan kerusakan pada sistem, dan mengambil alih kontrol jaringan. Ransomware, khususnya, mengenkripsi data pengguna dan menuntut tebusan untuk memulihkannya, yang dapat menyebabkan kerugian besar bagi bisnis dan uang. Oleh karena itu, sangat penting untuk memahami jenis malware dan ransomware yang tersedia, teknik deteksi yang efektif, dan metode mitigasi yang dapat digunakan untuk melindungi jaringan komputer.r.(Anggrahito, Ibrahim, and Pramudito 2020).

Tujuan dari penelitian ini adalah untuk menemukan jenis malware dan ransomware yang paling berbahaya, metode deteksi terbaik, dan teknik mitigasi yang dapat digunakan untuk mengurangi kemungkinan serangan jaringan komputer. Salah satu manfaatnya adalah pengelola jaringan menerima petunjuk praktis untuk meningkatkan keamanan siber organisasi mereka.

LANDASAN TEORI

1. Malware

Software berbahaya, juga dikenal sebagai malware, adalah program kode yang digunakan oleh penyerang untuk merusak atau menyalahgunakan sistem [4]. Terdapat berbagai

manacam jenis malware, tetapi fokus penelitian kami adalah malware jenis ransomware. Jenis malware ini bertujuan untuk menyimpan data atau akses ke sistem atau sumber daya dan kemudian menyimpannya di tangan sandera sampai korban membayar uang tebusan. Jenis malware ini juga menggunakan horses Trojan, backdoors, remote access Trojans, information stealers, Ransomware, Scareware, Fakeware, dan Greyware.(Prakasa 2020)

2. Ransomware

Serangan ransomware dapat mengganggu operasi bisnis dengan mengenkripsi data penting dan menuntut pembayaran untuk pemulihannya. Serangan ransomware yang terkenal seperti WannaCry dan NotPetya telah menunjukkan betapa berbahayanya ancaman ini.

METODE PENELITIAN

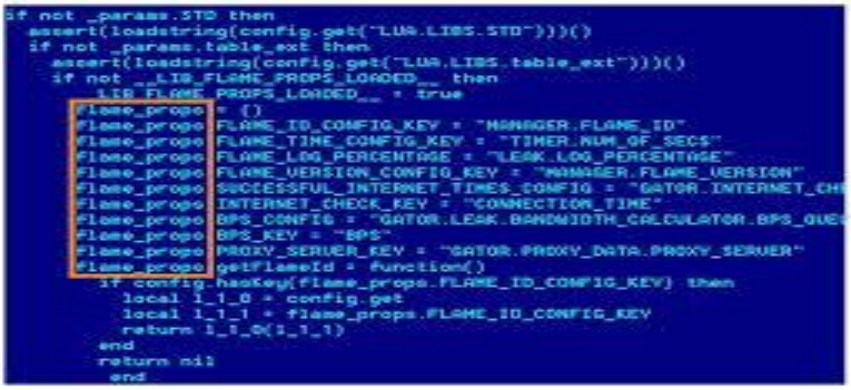
Dua pendekatan utama digunakan dalam penelitian ini. Pertama, studi literatur digunakan untuk mengumpulkan data tentang berbagai jenis malware dan ransomware, teknik deteksi, dan metode mitigasi yang telah diuji dan diterapkan. Kedua, eksperimen simulasi digunakan untuk menguji efektifitas strategi mitigasi yang disarankan dalam studi literatur dalam skenario kontrol yang terkendali.

PEMBAHASAN

1. Jenis malware dan ransomware yang paling umum dan berbahaya bagi jaringan komputer
   a. jenis malware
      1) Virus: Program yang dapat menggandakan dirinya sendiri dan menyebar ke komputer lain, sering merusak data atau sistem.

Gambar 1. Virus

      2) Worms: Seperti virus, tetapi dapat menyebar secara otomatis melalui jaringan tanpa interaksi pengguna.

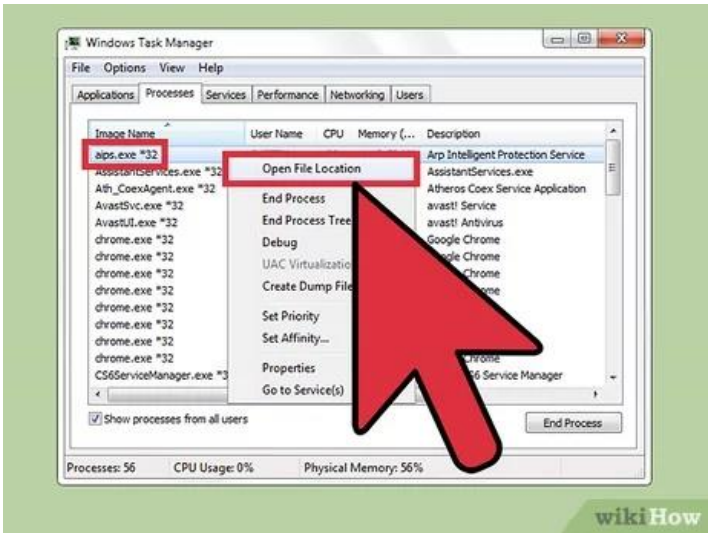


Gambar 2. Worms

3) Trojans: Program berbahaya yang menyamar sebagai software yang sah untuk mengelabui pengguna agar menginstalnya.

Gambar 3. Tojans

4) Spyware: Perangkat lunak yang mengumpulkan informasi pengguna tanpa sepengetahuan mereka.



Gambar 4. Spyware

b. Jenis Ransomware yang umum dan Berbahaya
   1) Crypto Ransomware: Mengenkripsi data pengguna dan menuntut tebusan untuk kunci dekripsi.
   2) Locker Ransomware: Mengunci akses pengguna ke sistem atau perangkat, menuntut tebusan untuk membuka kunci.
   3) Scareware: Mengelabui pengguna dengan ancaman palsu untuk membeli software yang tidak diperlukan atau berbahaya.

2. Metode deteksi yang efektif untuk mengindentifikasi serangan malware dan ransomware
   a. Antivirus dan Anti-malware Software

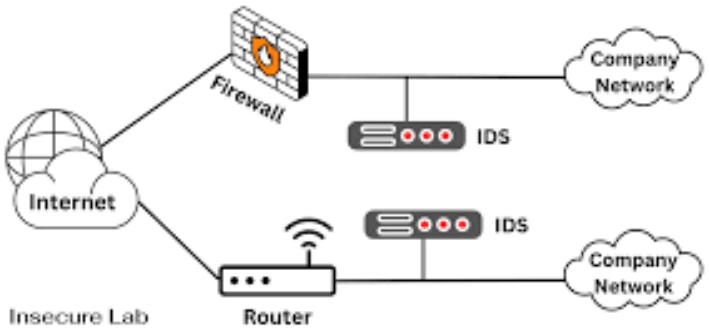
      Menggunakan database signature untuk mengidentifikasi dan menghapus malware yang diketahui. Pemindaian berkala dan real-time untuk mendeteksi ancaman.

Gambar 5. Anti virus

b. Intrusion Detection Systems (IDS)

Network-based IDS (NIDS): Memantau lalu lintas jaringan untuk mendeteksi aktivitas mencurigakan

Host-based IDS (HIDS): Memantau aktivitas pada sistem individual untuk mendeteksi perubahan yang tidak sah



Gambar 6. IDS

c. Teknik mitigasi yang dapat digunakan untuk menghentikan dan menanggapi serangan malware dan ransomwarePatch Management

Memastikan semua perangkat lunak dan sistem operasi diperbarui dengan patch keamanan terbaru untuk mencegah eksploitasi kerentanan yang diketahui.Backup dan RecoveryMelakukan backup data secara rutin dan menyimpan salinan di lokasi yang aman untuk memastikan data dapat dipulihkan setelah serangan ransomware.

d. Network Segmentation

Memisahkan jaringan ke dalam segmen-segmen yang lebih kecil untuk membatasi penyebaran malware jika terjadi infeksi.

e. User Education dan Awareness

Mengedukasi pengguna tentang praktik keamanan terbaik, seperti mengenali email phishing, menggunakan password yang kuat, dan tidak mengunduh perangkat lunak dari sumber yang tidak terpercaya.

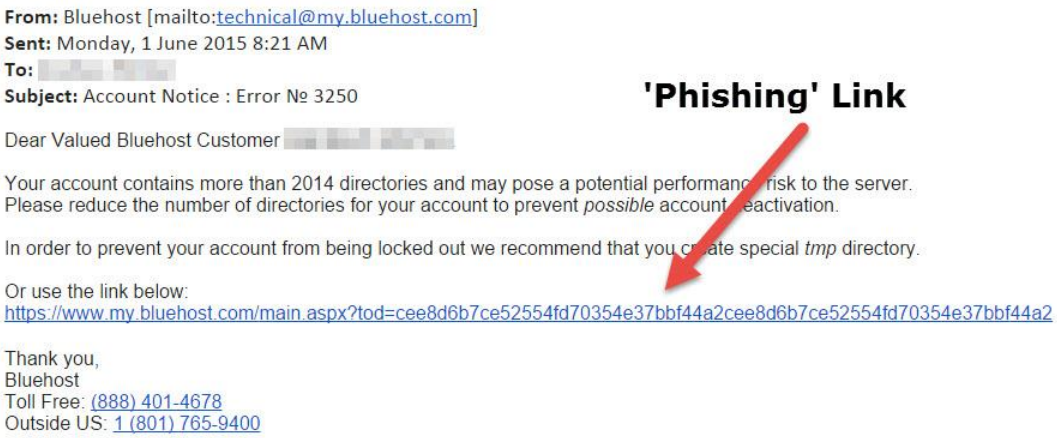
3. Simulasi

a. Alur Kerja Ransomeware

1) Kompromi awal

Seperti yang dinyatakan dalam laporan Verizon, metode paling umum untuk mengirimkan ransomware melalui email phishing. Beberapa skema phishing, seperti yang terbaru yang menargetkan Microsoft 365 melalui autentikasi multifaktor (MFA),

mengandung lampiran atau tautan berbahaya yang akan memulai pengunduhan ransomware ketika mereka diklik. Email ini dapat sangat menipu dan mendorong pengguna untuk melakukan hal-hal, seperti meminta permintaan mendesak dari kontak yang dikenal. Salah satu strategi ransomware yang sering digunakan adalah kit eksploitasi pada situs web yang disusupi, yang memindai bug sistem pengguna dan menggunakan bug ini untuk memasukkan ransomware. Karena ransomware hanya perlu mengunjungi halaman yang telah disusupi, strategi ini sangat bergantung pada tindakan pengguna.(Saputra, Deris, and Tata 2023)



Gambar 7. Simulasi Email Masuk Berisi Virus Ransomeware

2) Instalasi runsomeware

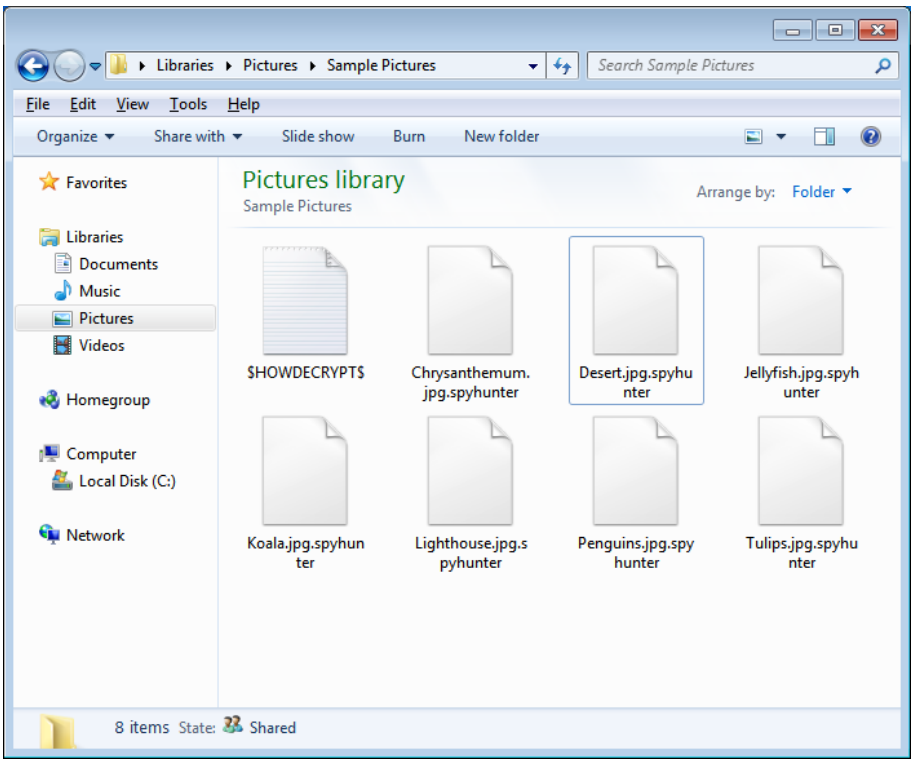
Setelah sistem disusupi, ransomware akan menginstal dirinya sendiri di komputer host. Kebanyakan ransomware menggunakan teknik untuk menghindari deteksi oleh perangkat lunak antivirus, seperti mengaburkan kode atau meniru proses perangkat lunak yang sah. Jenis ransomware tingkat lanjut mungkin juga mencoba meningkatkan hak istimewa dalam sistem untuk mendapatkan akses administratif. Jika hal ini terjadi, penjahat dunia maya dapat menjalankan perintah untuk menonaktifkan perangkat lunak keamanan Anda, mengubah proses sistem, dan memperluas jangkauan kerusakan yang ditimbulkannya

3) Penyebaran ransomeware

Beberapa varian ransomware dirancang untuk bergerak secara lateral di seluruh jaringan Anda, menginfeksi sistem dan server lain dalam organisasi Anda. Hal ini dapat menjadi skenario "terburuk" karena dapat mengakibatkan gangguan yang meluas dan peningkatan permintaan ransomware. Teknik propagasi berkisar dari mengeksploitasi kerentanan jaringan hingga mencuri kredensial untuk mendapatkan akses jaringan hingga secara jahat menggunakan alat manajemen jaringan yang sah

4) Enskripsi data

Setelah menyebar melalui sistem Anda, ransomware mengenkripsi file menggunakan algoritma enkripsi yang kuat seperti AES atau RSA. Setelah dienkripsi, file, database, aplikasi, dan seluruh sistem Anda mungkin tidak dapat diakses. Sayangnya, kunci enkripsi biasanya unik dan dipegang oleh peretas, membuat dekripsi hampir tidak mungkin dilakukan tanpa membayar uang tebusan



Gambar 8. Enskripsi data

5) Eksfiltaris data

Beberapa varian ransomware mengeksfiltrasi data Anda ke server yang dikendalikan oleh penyerang. Sebagaimana dicatat dalam Penasihat Keamanan Siber CISA baru-baru ini, Phobos Ransomware adalah salah satu contohnya. Hal ini membawa ancaman terhadap organisasi Anda ke tingkat yang lebih tinggi—sering disebut pemerasan ganda ransomware—karena penjahat dunia maya dapat mengancam untuk merilis informasi sensitif secara publik jika uang tebusan tidak dibayarkan. Hal ini merupakan tambahan dari masalah yang akan Anda alami saat data Anda dienkripsi

Gambar 9. Eksfiltaris data

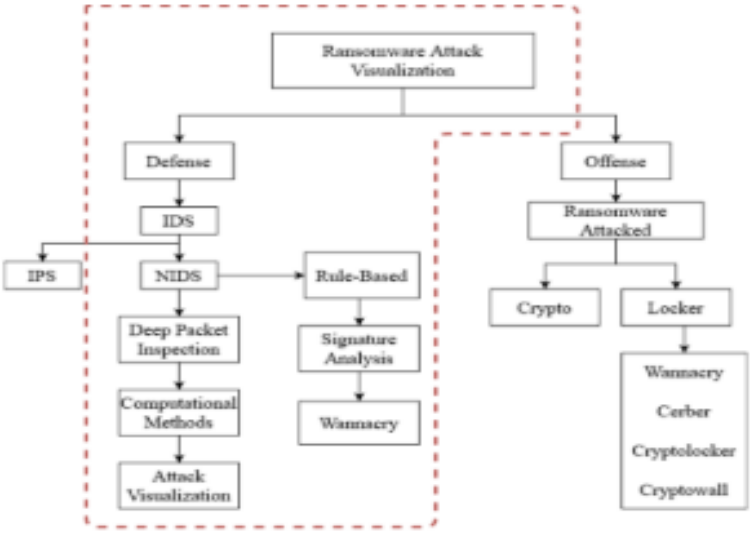
6) Tuntutan tebusan

Setelah data Anda dienkripsi—dan mungkin dieksfiltrasi—biasanya Anda akan menemukan catatan tebusan yang ditampilkan di perangkat atau sistem Anda. Catatan ini mencakup instruksi tentang cara membayar uang tebusan, biasanya dalam mata uang kripto seperti Bitcoin, dan mungkin berisi ancaman dan tenggat waktu untuk mendorong Anda membayar dengan cepat

Gambar 10. tuntutan tebusan

b. Metode deteksi malware runsomeware

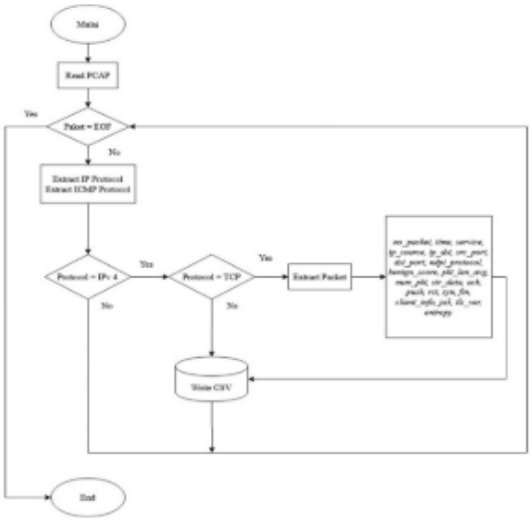
Diagram metode penelitian yang digunakan Snort dan Deep Packet Inspection dalam melakukan tindakan untuk mendeteksi Ransomware WannaCry ditunjukkan di bawah ini.



Gambar 11. diagram perancangan

Setelah mengidentifikasi ancaman Ransomware WannaCry, Deep Packet Inspection akan mengumpulkan data. Data dalam format .pcap akan dikumpulkan, tetapi format ini tidak dapat digunakan untuk mendapatkan informasi yang akurat; sebaliknya, Anda harus menjalani proses ekstraksi untuk mendapatkan informasi yang diinginkan. Tahapan selanjutnya adalah melakukan ekstraksi fitur. Proses ini akan menghasilkan hasil dalam bentuk data.xls yang dapat dibaca dan dipahami dan dapat divisualisasikan untuk

menjadi data yang matang dan siap digunakan. Gambar berikut menunjukkan alur kerja Feature Extraction.



Gambar 12. diagram perancangan

Setelah mengidentifikasi ancaman Ransomware WannaCry, Deep Packet Inspection akan mengumpulkan data. Informasi data serangan yang dilakukan: langkah selanjutnya adalah mengoreksi hasil deteksi DPI. Ini dilakukan dengan menggabungkan karakteristik serangan ransomware ke dalam pola serangan. Paket ransomware akan diklasifikasi dengan paket normal setelah memiliki fitur yang sesuai dengan jenis serangan. Untuk menguji total paket yang menjadi alert, algoritma visualisasi yang telah disediakan akan digunakan. Pada tahap terakhir, data paket akan divisualisasikan dalam bentuk diagram.

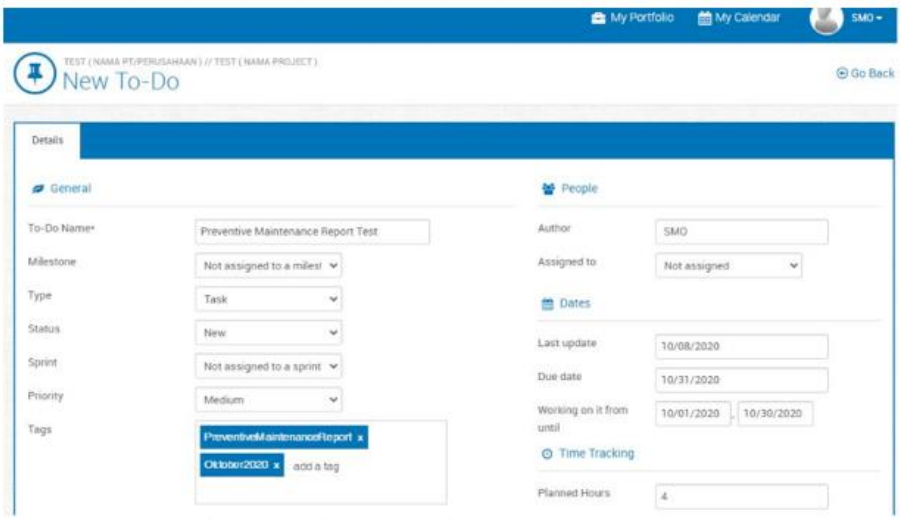
Selanjutnya, hasil ekstraksi akan digunakan untuk memvalidasi atribut yang dihasilkan oleh proses deteksi; waktu yang diperoleh akan divalidasi dengan atribut waktu.

Gambar 13. hasil deteksi

c. Strategi mitigasi

1) Patch Management

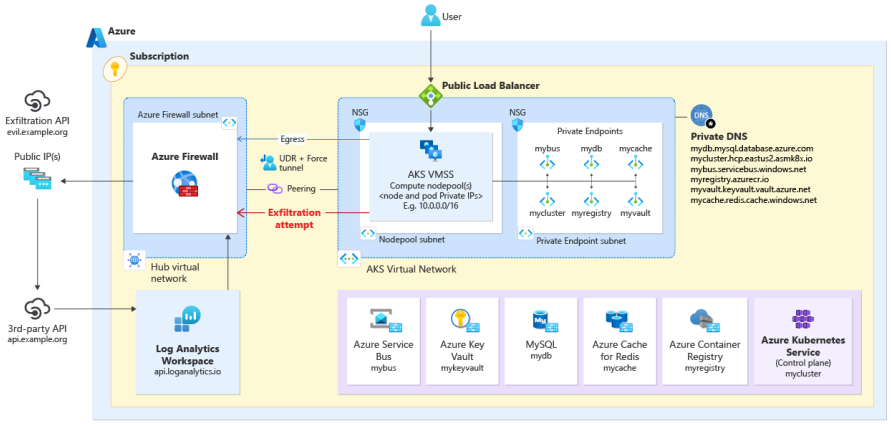
Penjelasan: Pastikan semua perangkat lunak dan sistem operasi diperbarui dengan patch keamanan terbaru untuk menutup kerentanan yang dapat dieksploitasi oleh ransomware.



Gambar 14. *patch management*

2) Network Segmentation

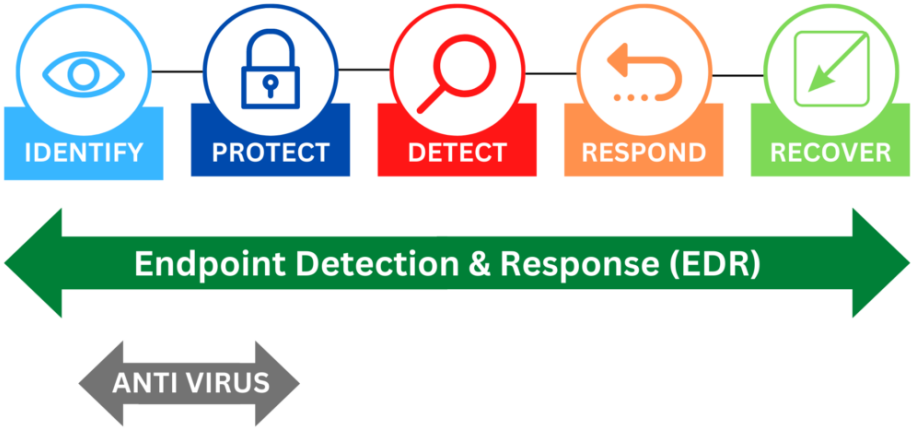
Penjelasan: Pisahkan jaringan ke dalam segmen-segmen yang lebih kecil untuk membatasi penyebaran ransomware jika terjadi infeksi.



Gambar 15. *Network segmentation*

3) Endpoint Detection and Response (EDR)

Penjelasan: Gunakan solusi EDR untuk memantau aktivitas endpoint secara real-time dan merespons ancaman dengan cepat



Gambar 16. Endpoint Detection Response (EDR)

KESIMPULAN DAN SARAN

Penelitian ini mengidentifikasi bahwa malware dan ransomware adalah ancaman serius bagi jaringan komputer. Metode deteksi yang efektif, seperti signature-based detection, heuristic analysis, behavioral analysis, machine learning, sandboxing, IDS, Snort, dan DPI, sangat penting dalam mendeteksi ancaman ini. Strategi mitigasi yang meliputi patch management, backup dan recovery, network segmentation, edukasi pengguna, penerapan software keamanan, rencana respons insiden, prinsip least privilege, dan EDR terbukti efektif dalam melindungi jaringan komputer dari serangan.(Saputra, Deris, and Tata 2023)

Organisasi disarankan untuk menerapkan solusi keamanan yang terintegrasi, termasuk antivirus, IDS, AI-based detection, dan EDR. Prosedur patch management harus diotomatisasi dan dilakukan secara rutin, sementara backup data perlu dilakukan secara berkala dan disimpan di lokasi aman. Program edukasi keamanan siber perlu ditingkatkan untuk membantu pengguna mengenali ancaman dan mengadopsi praktik keamanan yang baik. Penelitian lebih lanjut dan inovasi dalam teknologi keamanan, seperti penggunaan blockchain dan otomatisasi respons insiden, diperlukan untuk menghadapi ancaman yang semakin kompleks.

DAFTAR PUSTAKA

Anggrahito, Ramadhan Ibrahim, and Juliadi Satyo Pramudito. 2020. "Metode Cepat Identifikasi Dan Mitigasi Malware Ransomware Ketika Terjadi Serangan Siber Ramadhan Ibrahim." *Conference on Information Technology and Electrical Engineering* , 42–46.

Prakasa, Johan Ericka Wahyu. 2020. "Peningkatan Keamanan Sistem Informasi Melalui Klasifikasi Serangan Terhadap Sistem Informasi." *Jurnal Ilmiah Teknologi Informasi Asia* 14 (2): 75. https://doi.org/10.32815/jitika.v14i2.452.

Saputra, Dio Azmi, Stiawan Deris, and Sutabri Tata. 2023. "Implementasi Sistem Deteksi Ransomware Menggunakan Deep Packet Inspection Pada Layanan SMK Negeri 1 Palembang." *Indonesian Journal of Multidisciplinary on Social and Technology* 1 (2): 176–83. https://doi.org/10.31004/ijmst.v1i2.142.