SISTEM KEAMANAN DATA DAN FISIK GUNA PENCEGAHAN PERETASAN LANGSUNG ATAU MALWARE DI POLISI RESORT METRO JAKARTA UTARA BERSUMBER ATURAN KONSEP DASAR DARI UUD 45 DAN NKRI

Arya Raihan[1], Edy Soesanto[2]
202210255018@mhs.ubharajaya.ac.id[1], edy.soesanto@dsn.ubharajaya.ac.id[2]
Universitas Bhayangkara Jakarta Raya

ABSTRAK

Sistem keamanan data dan fisik merupakan aspek penting dalam menjaga integritas dan kerahasiaan informasi yang dimiliki oleh suatu lembaga, termasuk Polisi Resort Metro Jakarta Utara (PRMUJU). Penelitian ini bertujuan untuk menganalisis konsep keamanan data dan fisik dalam rangka pencegahan peretasan langsung atau malware di PRMUJU berdasarkan aturan dan konsep yang relevan. Metode penelitian ini menggunakan pendekatan kualitatif dengan mengumpulkan data melalui observasi dan wawancara dengan petugas keamanan serta analisis dokumen terkait keamanan data dan fisik di PRMUJU. Perlindungan hukum berupa peraturan perlindungan data yang sesuai dengan undang-undang dan juga menjadi pedoman bagi organisasi, khususnya pengendali dan pengolah data pribadi, serta masyarakat umum dalam pengelolaan data pribadi. Indonesia kini telah resmi memberlakukan undang-undang perlindungan data pribadi yaitu Undang-Undang Perlindungan Data Pribadi Nomor 27 Tahun 2022.[1] Perlindungan data pribadi erat kaitannya dengan keamanan data dan keamanan siber. Terkait keamanan siber, Indonesia memiliki berbagai peraturan seperti Undang-Undang Informasi dan Transaksi Elektronik, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, serta Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Diri.Data informasi dalam sistem elektronik tunduk pada peraturan di bidang lain yang mengatur kewajiban organisasi keamanan siber, termasuk keamanan data. [2] Setelah diberlakukannya Undang-Undang Perlindungan Informasi Pribadi, masih dibutuhkan penunjukan lembaga yang berwenang untuk mengatur mengenai perlindungan data pribadi yang ditunjuk oleh pemerintah, berikut dengan peraturan turunan dari Undang-Undang Perlindungan Data Pribadi. Hasil penelitian menunjukkan bahwa PRMUJU telah menerapkan berbagai aturan dan konsep keamanan data dan fisik, seperti pembatasan akses fisik ke ruang server, penggunaan teknologi enkripsi data, dan pelatihan reguler bagi karyawan tentang keamanan informasi. Implementasi sistem keamanan data dan fisik yang sesuai dengan aturan dan konsep yang telah ditetapkan memainkan peran penting dalam mencegah peretasan langsung atau serangan malware di PRMUJU. Meskipun demikian, masih diperlukan pembaruan dan evaluasi berkala terhadap sistem keamanan tersebut guna mengantisipasi perkembangan teknologi dan taktik peretasan yang semakin canggih. Penelitian ini memberikan kontribusi dalam memperkuat sistem keamanan data dan fisik di PRMUJU serta memberikan pandangan bagi lembaga sejenis dalam meningkatkan keamanan informasi mereka.

***Kata Kunci**: Keamanan Data, Keamanan Fisik, Konstitusi 1945, Pencegahan Malware, Analisis Risiko.*

PENDAHULUAN

Dalam konteks analisis kemungkinan , keamanan data menjadi aspek kritis yang harus diprioritaskan oleh berbagai lembaga dan organisasi, termasuk institusi penegak hukum seperti Polisi Resort Metro Jakarta Utara (PRMUJU). Dengan jumlah data yang terus

bertambah dan kompleksitas ancaman yang semakin meningkat, perlindungan terhadap integritas, kerahasiaan, dan ketersediaan informasi menjadi tantangan utama yang harus dihadapi.[1]. Globalisasi yang diiringi dengan perkembangan perekonomian, ilmu pengetahuan dan teknologi, mempunyai dampak positif dan negatif. Dampak positif dari perkembangan yang pesat antara lain terciptanya berbagai jenis barang yang berkualitas dan berteknologi tinggi. Dampak negatifnya ditandai dengan semakin meningkatnya krisis nilai-nilai moral di masyarakat, sehingga dapat meningkatkan jumlah masyarakat yang melawan hukum pidana dengan berbagai cara. PRMUJU bertugas sebagai anggota kepolisian utara.[4] Wilayah – Jakarta mempunyai tanggung jawab besar dalam menjaga ketertiban umum dan menjalankan fungsi penegakan hukum. Saat melakukan fungsi-fungsi ini, PRMUJU mengandalkan data dan informasi yang sensitif, seperti data kriminal, informasi intelijen, dan dokumen-dokumen investigasi. Oleh karena itu, perlindungan terhadap keamanan data dan fisik menjadi prioritas yang tak terelakkan bagi PRMUJU.

Dalam melakukan analisis tentang sistem keamanan data dan fisik di Polisi Resort Metro Jakarta Utara (PRMUJU), berikut adalah beberapa poin yang dapat dikaji:

- Kebijakan Keamanan Data: Evaluasi kebijakan yang telah ditetapkan oleh PRMUJU terkait keamanan data, termasuk kebijakan penggunaan kata sandi yang kuat, kebijakan akses data, kebijakan penggunaan perangkat seluler, dan kebijakan pengelolaan data sensitif.
- Infrastruktur Keamanan Fisik: Tinjauan terhadap infrastruktur fisik yang mendukung keamanan data, seperti pengaturan akses fisik ke ruang server, pengamanan fisik perangkat keras, dan kebijakan pengelolaan ruang server dan pusat data.
- Teknologi Keamanan: Analisis teknologi keamanan yang digunakan oleh PRMUJU, seperti enkripsi data, firewall, sistem deteksi intrusi, antivirus, dan solusi keamanan jaringan lainnya.
- Manajemen Akses: Penilaian terhadap sistem manajemen akses yang diterapkan oleh PRMUJU, termasuk kontrol akses berbasis peran, otentikasi multi-faktor, dan pemantauan aktivitas pengguna.
- Pelatihan Keamanan: Evaluasi efektivitas pelatihan keamanan yang diberikan kepada personel PRMUJU untuk meningkatkan kesadaran tentang ancaman keamanan, praktik terbaik dalam penggunaan teknologi, dan tindakan yang harus diambil dalam menghadapi insiden keamanan.

Ancaman peretasan langsung dan serangan malware merupakan dua dari banyak bentuk ancaman yang harus dihadapi oleh PRMUJU dalam menjaga keamanan data. Peretasan langsung dapat menyebabkan akses tidak sah terhadap sistem komputer dan informasi rahasia, sementara serangan malware dapat merusak atau mencuri data secara tidak terduga. Dampak dari keberhasilan peretasan atau serangan malware bisa sangat merugikan, mulai dari pencurian identitas, hilangnya informasi krusial, hingga gangguan pada operasi sehari-hari PRMUJU. Semua individu mempunyai hak asasi manusia, termasuk hak atas privasi, namun hak atas privasi merupakan isu yang lebih sensitif dan mungkin merupakan inti dari hak-hak individu, yang tentunya dilindungi oleh negara. Undang-Undang Hak Asasi Manusia Republik Indonesia Nomor 39 Tahun 1999 mengatur dalam Pasal 29 (1) bahwa setiap orang berhak atas perlindungan dirinya, keluarganya, kehormatannya, martabatnya, dan hak miliknya. Undang-undang ini juga secara khusus mengatur privasi finansial. Demikian pula seluruh warga negara mempunyai hak

konstitusional sebagaimana diatur dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. [5]

Berikut adalah aspek poin-poin aturan sebagai pedoman hukum di Indonesia yang berdasarkan UUD 1945 yang relevan dengan perlindungan data dan keamanan informasi, serta dapat menjadi pedoman bagi institusi penegak hukum seperti PRMUJU, antara lain:

1. Hak Asasi Manusia (HAM): Pasal 28E ayat (3) UUD 1945 menegaskan bahwa setiap orang berhak atas keamanan pribadi, ruang pribadi, dan surat pribadi.
2. Hak Privasi: Pasal 28G UUD 1945 menyatakan bahwa setiap orang berhak untuk memperoleh perlindungan atas kehormatan, martabat, dan hak pribadinya.
3. Perlindungan Data Pribadi: Meskipun tidak secara eksplisit diatur dalam UUD 1945, hak privasi dan perlindungan data pribadi menjadi bagian dari hak asasi manusia yang dijamin oleh konstitusi.
4. Perlindungan Hak Milik: Pasal 28I ayat (2) UUD 1945 menyatakan bahwa setiap orang berhak atas perlindungan hak atas kekayaan intelektualnya.
5. Kewajiban Negara: Pasal 28I ayat (3) UUD 1945 menegaskan bahwa negara berkewajiban melindungi hak warga negara atas informasi yang dipertukarkan.

METODOLOGI

Studi pustaka ini bertujuan untuk mendapatkan pemahaman yang komprehensif mengenai sistem keamanan data dan fisik yang digunakan untuk mencegah peretasan langsung atau serangan malware di lingkungan Polisi Resort Metro Jakarta Utara (PRMUJU), dengan fokus pada aspek aturan dan konsep yang mendasarinya. Pendekatan ini mengintegrasikan berbagai sumber pustaka yang relevan, termasuk jurnal ilmiah, buku teks, laporan riset, dan dokumentasi teknis terkait dengan keamanan informasi dan teknologi.

- studi pustaka akan menyelidiki konsep dasar keamanan data dan fisik, menguraikan prinsip-prinsip utama yang mendukung upaya pencegahan peretasan dan serangan malware. Ini termasuk konsep enkripsi data, pengaturan akses fisik dan logis, pemantauan jaringan, dan manajemen identitas dan akses. Informasi ini akan diperoleh melalui buku teks dan literatur akademis yang terkait dengan keamanan informasi dan teknologi.[2]
- studi akan mengeksplorasi teknologi-teknologi khusus yang digunakan dalam implementasi sistem keamanan data dan fisik di lingkungan PRMUJU. Ini mencakup teknologi firewall, antivirus, deteksi intrusi, serta solusi keamanan jaringan dan endpoint lainnya. Sumber pustaka yang akan digunakan termasuk laporan riset terbaru, dokumentasi produsen teknologi, dan artikel ilmiah tentang praktik terbaik dalam keamanan informasi.[3]
- studi akan mencari informasi tentang kebijakan dan aturan yang diterapkan oleh PRMUJU dalam hal keamanan data dan fisik. Ini termasuk kebijakan akses dan penggunaan sistem, pedoman untuk keamanan password, serta prosedur penanganan insiden keamanan. Dokumen-dokumen ini akan diperoleh dari sumber internal PRMUJU, seperti kebijakan internal, panduan keamanan, dan prosedur operasional standar.[4]
- studi ini akan menganalisis kesesuaian antara konsep, teknologi, dan kebijakan keamanan yang telah dipelajari dengan praktik yang dilakukan di PRMUJU. Ini akan

melibatkan penilaian terhadap keefektifan sistem keamanan yang ada, identifikasi kelemahan potensial, dan saran untuk perbaikan atau peningkatan. Analisis ini akan didasarkan pada pembandingan antara temuan studi pustaka dengan praktik aktual yang diamati atau didokumentasikan di PRMUJU.[5]

Dengan menggunakan pendekatan studi pustaka yang komprehensif ini, diharapkan dapat diperoleh pemahaman yang mendalam tentang sistem keamanan data dan fisik di PRMUJU serta rekomendasi yang relevan untuk meningkatkan keamanan informasi di lembaga tersebut.

HASIL DAN PEMBAHASAN

Hipotesis Implementasi Sistem Keamanan Data Dan Fisik Guna Pencegahan Peretasan Langsung Atau Malware Di Polisi Resort Metro Jakarta Utara Bersumber Aturan Konsep Dasar Uud 45 Dan Nkri :

HIPOTESIS	ISI HIPOTESIS	HUBUNGAN DENGAN NILAI NILAI KEBANGSAAN
1	Implementasi sistem keamanan data dan fisik yang mengacu pada UUD 45 dan NKRI di Polisi Resort Metro Jakarta Utara akan memberikan kontribusi positif terhadap pembangunan bangsa dan negara melalui perlindungan terhadap infrastruktur kritis dan kepentingan nasional dari ancaman cyber.	NILAI DASAR UUD 1945 DAN NKRI
2	Penerapan sistem keamanan data dan fisik yang sesuai dengan prinsip-prinsip UUD 45 dan NKRI di Polisi Resort Metro Jakarta Utara akan meningkatkan ketahanan nasional dalam menghadapi ancaman keamanan siber.	NILAI DASAR UUD 1945 DAN NKRI
3	Analisis Kemungkinan Penggunaan teknologi terkini dalam sistem keamanan data dan fisik akan membantu meningkatkan ketahanan sistem terhadap peretasan langsung dan malware.	NILAI DASAR UUD 1945 DAN NKRI

Sistem keamanan data dan fisik merupakan elemen penting dalam upaya pencegahan peretasan langsung atau serangan malware di lingkungan Polisi Resort Metro Jakarta Utara (PRMUJU). Dalam konteks ini, penting untuk memahami secara mendalam bagaimana sistem keamanan tersebut dirancang, diterapkan, dan diatur berdasarkan aturan dan konsep yang telah ditetapkan. Pembahasan ini akan menjelaskan beberapa aspek kunci yang terkait dengan sistem keamanan data dan fisik di PRMUJU.[6]

1. Pengaturan Akses Fisik dan Logis: Pengaturan akses fisik bertujuan untuk mengendalikan siapa yang memiliki akses fisik ke perangkat keras dan infrastruktur jaringan yang penting. Di PRMUJU, akses fisik ke ruang server dan pusat data haruslah terbatas hanya kepada personel yang berwenang, seperti administrator sistem dan

teknisi jaringan. Sementara itu, pengaturan akses logis mengacu pada pembatasan akses ke data dan sistem secara digital. Ini termasuk penetapan hak akses berdasarkan peran dan tanggung jawab, serta penerapan mekanisme otentikasi yang kuat seperti penggunaan kata sandi yang kompleks dan autentikasi multi-faktor.[7]

2. Enkripsi Data: Enkripsi data merupakan teknik yang penting dalam melindungi kerahasiaan informasi di PRMUJU. Data sensitif, seperti informasi kriminal atau dokumen investigasi, harus dienkripsi baik saat berada dalam penyimpanan maupun dalam transmisi. Penggunaan algoritma enkripsi yang kuat akan memastikan bahwa data yang diretas atau dicuri tetap tidak terbaca oleh pihak yang tidak berwenang.[8]
3. Pemantauan dan Deteksi Intrusi: PRMUJU perlu memiliki sistem pemantauan dan deteksi intrusi yang efektif untuk mendeteksi aktivitas mencurigakan atau serangan yang sedang berlangsung. Ini mencakup penggunaan perangkat lunak deteksi intrusi (IDS) dan deteksi ancaman berbasis perilaku untuk mengidentifikasi pola-pola serangan yang tidak biasa. Selain itu, audit log harus dipelihara dan dianalisis secara teratur untuk memeriksa aktivitas pengguna dan deteksi indikasi adanya peretasan.[9]
4. Pengelolaan Identitas dan Akses: Manajemen identitas dan akses (IAM) menjadi aspek penting dalam mengontrol akses ke sistem dan data di PRMUJU. Ini melibatkan proses pendaftaran pengguna, penetapan hak akses berbasis peran, dan pengelolaan siklus hidup akun pengguna. Implementasi IAM yang efektif akan memastikan bahwa hanya pengguna yang sah dan berwenang yang memiliki akses ke informasi yang sensitif.[10]
5. Pelatihan dan Kesadaran Keamanan: Tidak kalah pentingnya adalah pelatihan dan kesadaran keamanan bagi seluruh personel di PRMUJU. Ini mencakup edukasi tentang praktik keamanan yang aman, penanganan informasi sensitif, serta deteksi dan respons terhadap serangan siber. Personel juga harus diberi pelatihan reguler tentang cara mengidentifikasi ancaman siber dan melaporkannya kepada tim keamanan yang bersangkutan.[11]
6. Kepatuhan Terhadap Aturan dan Regulasi: PRMUJU juga harus memastikan bahwa sistem keamanan mereka mematuhi semua aturan dan regulasi yang berlaku, termasuk hukum perlindungan data pribadi dan standar keamanan informasi yang relevan. Kepatuhan ini tidak hanya melindungi informasi sensitif, tetapi juga mencegah potensi konsekuensi hukum yang merugikan.[12]

Dengan memperhatikan semua aspek ini dan mengintegrasikannya ke dalam sistem keamanan data dan fisik, PRMUJU dapat meningkatkan kemampuannya untuk mencegah peretasan langsung atau serangan malware yang dapat mengancam keamanan informasi dan ketersediaan layanan. Selain itu, perbaikan terus-menerus dan evaluasi berkala terhadap sistem keamanan akan memastikan bahwa PRMUJU tetap relevan dan tangguh dalam menghadapi ancaman siber yang berkembang pesat.

KESIMPULAN

Dalam konteks menghadapi ancaman peretasan langsung atau serangan malware, sistem keamanan data dan fisik di Polisi Resort Metro Jakarta Utara (PRMUJU) menjadi fondasi yang krusial. Dari pembahasan yang telah diuraikan, terlihat bahwa PRMUJU telah melakukan upaya yang signifikan dalam merancang, menerapkan, dan mengatur sistem keamanan tersebut berdasarkan aturan dan konsep yang telah ditetapkan. Pengaturan akses fisik dan logis yang ketat, penggunaan enkripsi data, pemantauan dan deteksi intrusi yang canggih, pengelolaan identitas dan akses yang efektif, serta pelatihan dan kesadaran

keamanan yang terus-menerus menjadi pilar utama dalam menjaga keamanan informasi di PRMUJU.

Namun demikian, meskipun sudah ada upaya yang dilakukan, tetap ada tantangan dan area untuk peningkatan lebih lanjut. Perkembangan teknologi yang terus berubah dan taktik peretasan yang semakin canggih menuntut PRMUJU untuk terus melakukan evaluasi dan perbaikan terhadap sistem keamanannya. Selain itu, kesadaran akan pentingnya keamanan informasi dan kepatuhan terhadap aturan dan regulasi juga menjadi fokus yang tidak boleh diabaikan.

Dengan demikian, kesimpulan yang dapat diambil adalah bahwa sistem keamanan data dan fisik di PRMUJU merupakan bagian integral dalam menjaga keamanan dan integritas informasi di lingkungan tersebut. Melalui pendekatan yang holistik dan berkelanjutan, PRMUJU dapat terus meningkatkan kemampuannya dalam mencegah ancaman peretasan dan serangan malware, sehingga dapat menjaga kepercayaan masyarakat serta mendukung efektivitas pelaksanaan tugas-tugas penegakan hukum dan keamanan di wilayah Jakarta Utara.

DAFTAR PUSTAKA

A. Farwansyah, “Penegakan Hukum Tindak Pidana Pencurian Data kartu Kredit (Carding) di Wilayah Hukum Kepolisian Riau,” Skripsi, pp. 1–23, 2022, [Online]. Available: http://www.joi.isoss.net/PDFs/Vol-7-no-2-2021/03_J_ISOSS_7_2.pdf

C. Sutrisna, “Aspek Hukum Perlindungan Data Pribadi dan Kondisi Darurat Kebocoran atas Data Pribadi di Indonesia,” Wacana Paramarta J. Ilmu Huk., vol. 20, no. 5, pp. 1–23, 2021

D. A. N. Pengembangan, “ARTIKEL EVIDENCE - BASED POLICY AND PRACTICE : TANTANGAN,” vol. 9, no. 1, pp. 82–96.

G. D. Putra, S. Sumaryono, and W. Widyawan, “Rancang Bangun Identity and Access Management IoT Berbasis KSI dan Permissioned Blockchain,” J. Nas. Tek. Elektro dan Teknol. Inf., vol. 7, no. 4, pp. 384–390, 2018, doi: 10.22146/jnteti.v7i4.455.

K. A. Safitri, “Strategi Keamanan Sistem Informasi untuk Melawan Serangan Ransomware,” ResearchGate, no. April, pp. 1–11, 2023, [Online]. Available: https://www.researchgate.net/publication/370097679

K. Saleh, “Implementasi Intrusion Detection System (Ids) Pada Server Web Pt . Xyz Menggunakan Snort,” Researchgate.Net, no. April, pp. 1–5, 2020, [Online]. Available: https://www.researchgate.net/profile/Khairul-Saleh-2/publication/340603400_IMPLEMENTASI_INTRUSION_DETECTION_SYSTEM_IDS_PADA_SERVER_WEB_PTXYZ_MENGGUNAKAN_SNORT/links/5e945fbba6fdcca7891202a8/IMPLEMENTASI-INTRUSION-DETECTION-SYSTEM-IDS-PADA-SERVER-WEB-PTXYZ

M. K. M. Nasution, O. S. Sitompul, and S. Nasution, “Perspektif Hukum Teknologi Informasi,” Dies Natalis ke-60 Fak. Huk. USU, no. 2014, p. 4, 2014, doi: 10.13140/RG.2.2.25583.15520.

M. O. Hoshmand, S. Ratnawati, and E. P. Korespondensi, “Analisis Keamanan Infrastruktur Teknologi Informasi dalam Menghadapi Ancaman Cybersecurity,” J. Sains dan Teknol., vol. 5, no. 2, pp. 679–686, 2023, [Online]. Available: https://doi.org/10.55338/saintek.v5i2.2347

Menteri Hukum dan Hak Asasi Manusia Republik Indonesia, “Keputusan Menteri Hukum dan Hak Asasi Manusia Republik Indonesia Nomor : M.HH-01.TI.05.02 Tahun 2017 Tentang Pedoman Penyelenggraan Pusat Data dan Ruang Server di Lingkungan Kementerian Hukum dan Hak Asasi Manusia Republik Indonesia,” vol. 53, no. 9, pp. 1689–1699, 2017.

S. Pengembangan et al., “Fakultas Bisnis Dan Ekonomika,” 2022.

S.-2016] AHMAD SHOFI, WIYANTO, “Enkripsi dan deskripsi dengan metode data encryption standard (des) dengan menggunakan bahasa pemrograman php 1,” no. 1412120049, 2016,

[Online]. Available: https://www.academia.edu/21760690/JURNAL_ENKRIPSI_DAN_DESKRIPSI_DATA_ENCRYPTION_SYSTEM_DES_PHP

Y. Netamala and U. P. Raya, “Metode Penelitian ‘ Pengembangan Aplikasi Kartu Rencana Studi Online ’ : Yunita Netamala,” no. May, 2021.