Jurnal Mahasiswa Komunikasi CANTRIK
E-ISSN: 2807-2499
Volume 4, Nomor 2, 2024, Hal 93-102
DOI: 10.20885/cantrik.vol4.iss2.art2
Article History | Submitted: August 10, 2024 | Accepted: Nov 30, 2024 | Published: Nov 30, 2024

Peran Regulasi Komunikasi dalam Mengatasi Pencurian Data Nasional pada 2024

The Role of Communication Regulations in Overcoming National Data Theft in 2024

Muhammad Farrel Tanjung [1*] & Fadilla Febrianisa [2]
[1,2]Universitas Islam Indonesia, Yogyakarta, Indonesia
*Penulis Korespondensi

Author's email:
[1]fareltanjung15@gmail.com

Keywords:
cyber communication regulation, password, cyber attacks, national data security.

Abstract: *This study examines the impact of national data theft by hackers in 2024 by identifying weak communication regulations. The study was conducted using a qualitative approach with a case strategy. The study results found the need for strict regulations to protect sensitive data by emphasizing that clear and consistently implemented policies can reduce the risk of data theft. The case studies analyzed showed that weak passwords significantly increased vulnerability to attacks, illustrating the need for better education and implementation of stronger security practices. In conclusion, this study underscores the importance of effective regulations in addressing cyber threats and improving the protection of personal information in today's digital era.*

Kata kunci:
regulasi komunikasi siber, kata sandi, serangan siber, keamanan data nasional.

Abstrak: Penelitian ini mengulas dampak pencurian data nasional oleh hacker pada 2024 dengan mengidentifikasi lemahnya regulasi komunikasi. Penelitian dilakukan dengan menggunakan pendekatan kualitatif dengan strategi kasus. Hasil penelitian menemukan perlunya regulasi yang ketat untuk melindungi data sensitif dengan menekankan bahwa kebijakan yang jelas dan diterapkan secara konsisten dapat mengurangi risiko pencurian data. Studi kasus yang dianalisis menunjukkan bahwa penggunaan kata sandi yang lemah secara signifikan meningkatkan kerentanan terhadap serangan, mengilustrasikan perlunya edukasi yang lebih baik dan implementasi praktik keamanan yang lebih kuat. Kesimpulannya, penelitian ini menggarisbawahi pentingnya peraturan yang efektif dalam menanggulangi ancaman siber dan meningkatkan perlindungan terhadap informasi pribadi di era digital saat ini.

PENDAHULUAN

Pada 2024, terjadi peningkatan signifikan dalam insiden pencurian data nasional yang disebabkan oleh hacker. Peningkatan ini menunjukkan bahwa meskipun teknologi dan langkah-langkah keamanan terus berkembang, para hacker juga semakin canggih dalam mengeksploitasi kelemahan sistem. Salah satu faktor utama yang ditemukan dalam serangkaian insiden ini adalah penggunaan kata sandi yang sangat lemah, seperti "Admin#1234" (Andhika, 2024). Kata sandi semacam ini sangat mudah ditebak dan dieksploitasi oleh peretas menggunakan teknik sederhana seperti *brute force attack* atau *credential stuffing*. Kerentanan ini menunjukkan bahwa meskipun kesadaran tentang pentingnya kata sandi yang kuat telah ada sejak lama, implementasinya masih jauh dari memadai di banyak organisasi.

Regulasi komunikasi yang ada saat ini tampaknya belum efektif dalam mengatasi masalah keamanan ini. Banyak regulasi yang ada tidak secara spesifik mengatur tentang penggunaan kata sandi yang kuat atau praktik terbaik dalam manajemen kata sandi. Misalnya, beberapa regulasi mungkin hanya memberikan panduan umum tentang perlindungan data tanpa menekankan pentingnya aspek teknis tertentu seperti otentikasi dua faktor atau enkripsi yang kuat. Akibatnya, organisasi yang mematuhi regulasi tersebut masih mungkin memiliki celah keamanan yang dapat dieksploitasi oleh peretas. Selain itu, ketidakefektifan regulasi ini juga dapat disebabkan oleh kurangnya penegakan hukum yang tegas dan konsisten, serta keterbatasan dalam sumber daya dan infrastruktur yang dibutuhkan untuk mendukung kepatuhan terhadap regulasi. Oleh karena itu, penting untuk mengevaluasi hubungan antara regulasi komunikasi dan keamanan data guna mengembangkan strategi yang lebih baik dalam melindungi informasi sensitif. Evaluasi harus mencakup analisis menyeluruh tentang bagaimana regulasi yang ada diterapkan dan di mana letak kekurangannya. Misalnya, regulasi perlu memperjelas standar minimum untuk kekuatan kata sandi dan mengharuskan penggunaan teknologi otentikasi tambahan yang dapat memberikan lapisan perlindungan ekstra. Selain itu, regulasi harus mendorong organisasi untuk secara rutin mengaudit sistem keamanan mereka dan melakukan pelatihan bagi karyawan tentang praktik keamanan siber yang baik. Lebih lanjut, evaluasi juga harus mempertimbangkan bagaimana regulasi komunikasi dapat diselaraskan dengan perkembangan teknologi dan ancaman siber yang terus berubah. Ini mungkin memerlukan pembaruan regulasi yang lebih sering serta penyesuaian cepat terhadap metode baru yang digunakan oleh peretas. Regulasi juga harus mempromosikan kerja sama antara sektor publik dan swasta dalam berbagi informasi tentang ancaman dan praktik terbaik dalam keamanan siber.

Dengan mengevaluasi dan memperbarui regulasi komunikasi secara menyeluruh, kita dapat mengembangkan strategi yang lebih efektif untuk melindungi data sensitif dan mengurangi risiko pencurian data di masa depan. Perlindungan yang lebih baik terhadap data pribadi dan informasi sensitif tidak hanya akan meningkatkan kepercayaan publik terhadap sistem digital, tetapi juga memberikan landasan yang lebih kuat bagi perkembangan teknologi dan ekonomi digital yang aman.

Penelitian terdahulu yang dilakukan oleh Bahtiar (2022) mengkaji regulasi perlindungan data pribadi di Indonesia dan mengidentifikasi kendala-kendala yang dihadapi dalam implementasinya. Metode yang digunakan dalam penelitian ini adalah analisis dokumen dan wawancara mendalam dengan para ahli di bidang regulasi data dan keamanan siber. Hasil penelitiannya menunjukkan bahwa regulasi perlindungan data pribadi di Indonesia masih lemah dan belum komprehensif, yang ditandai dengan belum disahkannya Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP). UU ITE yang saat ini berlaku juga belum mampu memberikan perlindungan yang optimal. Kekurangan regulasi ini diperparah

oleh kurangnya pemahaman dan komitmen dari berbagai pihak, termasuk pemerintah dan sektor swasta, terhadap pentingnya perlindungan data pribadi. Penelitian menyimpulkan perlunya penguatan regulasi dan peningkatan kesadaran masyarakat mengenai pentingnya perlindungan data pribadi.

Penelitian Nugroho et al. (2023) mengevaluasi kinerja tiga perangkat lunak password cracker, yaitu John The Ripper, Hashcat, dan Zydra, dalam melakukan serangan *brute force* pada berkas ZIP yang diamankan dengan sandi. Penelitian ini menyoroti efektivitas serangan *brute force*, yang mencoba setiap kemungkinan kombinasi kata sandi, khususnya pada sandi pendek yang lebih rentan dibobol. Hasil penelitian menunjukkan bahwa panjang kata sandi sangat mempengaruhi tingkat kesulitan dalam membobol file. Semakin kompleks kombinasi huruf, angka, dan simbol, semakin sulit pula proses peretasannya. Kesimpulan dari penelitian ini adalah pentingnya penggunaan kata sandi yang kuat dan kompleks untuk meningkatkan keamanan data digital. Penelitian ini juga merekomendasikan penggunaan alat pengujian seperti Hashcat, yang memiliki efektivitas tinggi dalam serangan brute force dengan tingkat keberhasilan memuaskan. Perbedaan dengan penelitian yang akan dilakukan adalah bahwa Nugroho et al. berfokus pada evaluasi teknis perangkat lunak untuk serangan password, sementara penelitian ini lebih mengarah pada peran regulasi komunikasi dalam konteks nasional. Namun, keduanya menekankan pentingnya keamanan data di era digital sebagai isu yang mendesak untuk ditangani

Rianto (2019) mengkaji paradigma regulasi di Indonesia. Studinya menemukan bahwa meskipun regulasi di Indonesia menginduk pada undang-undang dasar, tetapi ternyata paradigma berbeda-beda. Paradigma regulasi pers adalah demokrasi, film tidak demokratis, sedangkan penyiaran semi demokratis. Salah satu indikatornya adalah kebijakan negara dalam hal sensor.

Sarjito (2024) menggunakan pendekatan kualitatif dengan analisis data sekunder, mengkaji regulasi perlindungan data seperti GDPR dan dampaknya terhadap keamanan data pemerintah di era digital. Tujuan penelitian ini untuk mengeksplorasi tantangan dan strategi yang dihadapi pemerintah dalam melindungi data sensitif, termasuk pengaruh serangan siber terhadap kepercayaan publik dan operasional pemerintahan. Hasil penelitiannya menunjukkan bahwa serangan siber, seperti kasus SolarWinds, tidak hanya mengganggu operasi pemerintahan, tetapi juga merusak kepercayaan publik terhadap kemampuan pemerintah dalam melindungi data pribadi. Studi ini juga menyoroti pentingnya evaluasi regulasi secara berkelanjutan untuk mengatasi ancaman keamanan yang terus berkembang, serta perlunya keseimbangan antara transparansi dan keamanan data dalam inisiatif keterbukaan data.

Perbedaan utama penelitian ini dengan penelitian Sarjito dan juga penelitian-penelitiannya adalah pada evaluasi regulasi dan dampaknya terhadap kepercayaan publik, sedangkan penelitian ini lebih menekankan pada peran regulasi komunikasi dalam menghadapi pencurian data nasional. Penelitian ini sejalan dengan pandangan bahwa pendekatan yang adaptif dan komprehensif sangat diperlukan untuk memastikan keamanan data yang efektif. Oleh karena itu, penelitian ini dilakukan untuk menginvestigasi kebijakan keamanan data dan keberadaan kata sandi. Penelitian ini diharapkan memberikan kontribusi dalam studi regulasi komunikasi yang belum banyak dikerjakan, dan lebih memberikan pemahaman yang lebih baik bagi keamanan data.

KERANGKA TEORI

Teori regulasi komunikasi dalam konteks keamanan siber, khususnya dalam mengatasi pencurian data nasional, merupakan elemen kunci yang harus dipahami secara mendalam. Regulasi komunikasi merujuk pada pengaturan formal yang dibuat oleh lembaga

pemerintah atau otoritas terkait untuk mengatur bagaimana informasi disebarkan, ditransmisikan, dan dilindungi dalam suatu negara (Rianto, 2024). Dalam konteks keamanan data, regulasi komunikasi memainkan peran penting dalam menjaga integritas, kerahasiaan, dan ketersediaan data, terutama ketika data tersebut rentan terhadap ancaman seperti pencurian, kebocoran, atau serangan siber lainnya.

Definisi regulasi komunikasi dalam konteks ini adalah seperangkat aturan dan kebijakan yang dirancang untuk mengelola cara komunikasi digital dikendalikan, dipantau, dan dilindungi (Feintuck & Varney, 2006). Regulasi ini mencakup berbagai aspek, termasuk kebijakan keamanan siber, pengawasan lalu lintas data, hingga mekanisme enkripsi untuk melindungi data sensitif dari akses yang tidak sah. Tujuan utama regulasi komunikasi adalah untuk memastikan bahwa informasi yang dikirimkan melalui jaringan komunikasi digital aman dan terlindungi dari berbagai ancaman eksternal maupun internal .

Variabel utama dalam teori regulasi komunikasi mencakup beberapa aspek kunci yang harus dipertimbangkan dalam pengembangan dan implementasi regulasi. Variabel pertama adalah kebijakan keamanan siber, yang mengacu pada aturan dan prosedur yang dirancang untuk melindungi data dari ancaman digital. Kebijakan ini mencakup regulasi terkait penggunaan enkripsi, pengelolaan akses, dan prosedur penanganan insiden siber. Li et al., (2019) menegaskan bahwa kesadaran akan kebijakan keamanan siber meningkatkan perilaku karyawan dalam melindungi data, sehingga kebijakan yang kuat menjadi fondasi bagi regulasi komunikasi yang efektif dalam mencegah ancaman digital.

Variabel kedua adalah pengawasan dan kepatuhan, yang mencakup upaya pemantauan aktivitas untuk memastikan regulasi ditaati dan diterapkan secara konsisten. Pengawasan yang terintegrasi memungkinkan deteksi dini terhadap ancaman siber, sehingga dapat mencegah kerugian lebih lanjut dan menjaga stabilitas sistem komunikasi sesuai dengan standar yang telah ditetapkan. Sarjito (2024) menegaskan bahwa pengawasan yang efektif memainkan peran penting dalam menjaga integritas data pemerintah, terutama di tengah meningkatnya ancaman siber yang kompleks dan lintas batas. Selain itu, pengawasan ini harus mencakup audit reguler terhadap sistem dan jaringan komunikasi untuk mengidentifikasi potensi kelemahan dan memastikan tindakan korektif dapat dilakukan segera. Penegakan hukum yang tegas dan konsisten juga menjadi bagian penting dalam memastikan bahwa semua pihak mematuhi regulasi, sehingga risiko pelanggaran dapat diminimalkan dan kepercayaan publik terhadap keamanan data pemerintah dapat terjaga.

Variabel ketiga adalah kesadaran dan edukasi, yang bertujuan meningkatkan pemahaman individu serta organisasi tentang pentingnya keamanan informasi. Dalam konteks regulasi komunikasi, variabel ini menjadi komponen penting untuk mendukung keamanan siber. Chaudhary et al., (2022) menekankan bahwa program kesadaran siber yang dirancang dengan baik dapat mendorong praktik keamanan yang lebih baik di tingkat organisasi. Metode terukur seperti pelatihan berbasis skenario dan evaluasi kinerja terbukti efektif dalam meningkatkan pemahaman individu terhadap ancaman siber. Selain itu, pendekatan edukasi berkelanjutan membantu memastikan karyawan tetap waspada terhadap ancaman baru yang terus berkembang. Dengan implementasi strategi yang tepat, kesadaran keamanan siber tidak hanya melindungi data organisasi dari ancaman tetapi juga memperkuat ketahanan siber, sehingga menciptakan lingkungan kerja yang lebih aman dan terjamin.

Variabel keempat adalah kolaborasi antar lembaga dan sektor, yang memainkan peran vital dalam membangun kebijakan keamanan siber yang efektif. Mishra et al. (2022) menekankan bahwa sinergi antara institusi pemerintah, sektor swasta, dan komunitas internasional sangat penting untuk memperkuat kerangka kerja keamanan siber

secara global. Kolaborasi ini tidak hanya memungkinkan berbagi informasi dan sumber daya, tetapi juga mempercepat respons terhadap ancaman siber melalui koordinasi yang lebih baik. Selain itu, kerja sama lintas sektor mendorong pengembangan standar keamanan global yang dapat memudahkan harmonisasi regulasi di berbagai negara. Dengan ancaman siber yang semakin kompleks dan lintas batas, kolaborasi menjadi kunci untuk mengintegrasikan strategi, memperkuat pertahanan kolektif, dan menciptakan ekosistem keamanan siber yang tangguh dan adaptif terhadap tantangan di masa depan.

Regulasi komunikasi menjadi sangat relevan dalam mengatasi pencurian data nasional karena pentingnya melindungi informasi sensitif yang berperan dalam keamanan negara. Dengan berkembangnya layanan berbasis data dan teknologi yang semakin kompleks, ancaman terhadap kerahasiaan, integritas, dan ketersediaan data menjadi semakin nyata. Sebagai contoh, kebocoran data dapat merusak kepercayaan publik dan membahayakan keamanan nasional, seperti yang ditunjukkan oleh beberapa insiden pelanggaran data di Negara Nepal pada awal 2024 (Adhikari, 2024). Regulasi yang kuat, seperti kebijakan keamanan siber, diperlukan untuk mengatur pengelolaan, perlindungan, dan akses terhadap data. Tanpa regulasi yang memadai, risiko pencurian data akan terus meningkat, membahayakan stabilitas nasional dan keamanan masyarakat

METODE

Metode penelitian yang diterapkan pada studi mengenai peran regulasi komunikasi dalam mengatasi pencurian data nasional menggunakan penelitian kualitatif dengan strategi kasus. Pendekatan ini melibatkan studi kepustakaan yang mencakup pengumpulan data sekunder dari berbagai sumber terpercaya, seperti buku, artikel jurnal, laporan penelitian, dan sumber berita terpercaya. Menurut Adnani (2021), studi kepustakaan bertujuan memberikan dasar teoritis yang kokoh serta pemahaman mendalam terhadap fenomena kompleks melalui analisis data sekunder.

Proses seleksi literatur dilakukan secara sistematis melalui penggunaan kata kunci yang relevan, peninjauan abstrak, dan verifikasi sumber dari database akademik serta penerbit resmi. Literasi yang dipilih meliputi jurnal-jurnal komunikasi yang membahas regulasi komunikasi, keamanan data, dan dampak terhadap ancaman siber. Langkah tersebut memastikan bahwa hanya sumber dengan kredibilitas tinggi serta relevansi kuat yang digunakan untuk proses analisis.

Analisis data dilakukan secara kualitatif dengan mengeksplorasi hubungan antara regulasi komunikasi dan kerentanan terhadap pencurian data. Kajian ini menyoroti bagaimana aspek kelemahan dalam penggunaan kata sandi serta tantangan implementasi strategi keamanan siber, sehingga diharapkan mampu menghasilkan rekomendasi kebijakan yang lebih efektif.

HASIL & PEMBAHASAN

Kebijakan Keamanan Siber

Dalam konteks pencurian data nasional, kebijakan keamanan siber menjadi landasan utama dalam melindungi informasi sensitif. Kebijakan mencakup protokol keamanan, regulasi enkripsi, serta standar operasional yang wajib diterapkan oleh berbagai organisasi. penelitian menemukan bahwa kelemahan dalam kebijakan keamanan, seperti minimnya regulasi penggunaan kata sandi yang kuat, telah berkontribusi pada insiden pencurian data. Contoh nyata adalah kasus penggunaan kata sandi "Admin#1234" yang menjadi titik lemah dalam serangkaian serangan siber. Kata sandi mudah ditebak melalui metode brute force, yang menunjukkan kurangnya pengawasan dan implementasi kebijakan keamanan yang memadai.

Kajian pustaka mendukung perlunya regulasi yang lebih spesifik. Li et al., (2019) menunjukkan bahwa kesadaran karyawan terhadap kebijakan keamanan siber meningkatkan perilaku protektif terhadap data.

Namun, tanpa aturan yang jelas, organisasi cenderung mengabaikan langkah-langkah kritis seperti otentikasi dua faktor dan enkripsi data. Penelitian menekankan bahwa regulasi yang mewajibkan penggunaan teknologi tersebut dapat secara signifikan mengurangi risiko pencurian data. Selain itu, regulasi harus dirancang untuk fleksibel mengikuti perkembangan ancaman siber yang terus berubah.

Regulasi keamanan siber juga perlu disertai mekanisme audit rutin dan penegakan hukum yang tegas. penelitian Sarjito (2024) menunjukkan bahwa pengawasan efektif dan regulasi adaptif sangat penting untuk menghadapi ancaman siber lintas batas. Dengan regulasi yang kuat, organisasi dapat memastikan implementasi praktik keamanan yang sesuai standar, sehingga menciptakan ekosistem digital yang lebih aman.

Pengawasan dan Kepatuhan

Pengawasan dan kepatuhan terhadap regulasi adalah komponen kunci dalam mengurangi risiko pencurian data. Penelitian menemukan bahwa banyak organisasi gagal mematuhi standar keamanan dasar, seperti pemantauan lalu lintas data dan pelaporan insiden siber secara tepat waktu. Kekurangan tersebut sering disebabkan oleh minimnya sumber daya atau kurangnya kesadaran akan pentingnya kepatuhan terhadap regulasi.

Pengawasan yang terintegrasi memungkinkan deteksi dini terhadap aktivitas mencurigakan. Misalnya, penemuan pola akses tidak wajar dapat membantu mencegah serangan sebelum data berhasil dicuri. Penelitian Sarjito (2024) menegaskan pentingnya audit reguler dan penegakan hukum untuk memastikan standar keamanan terpenuhi. Selain itu, pengawasan perlu dilengkapi dengan teknologi otomatis, seperti sistem deteksi intrusi berbasis AI, yang dapat mengidentifikasi ancaman secara *real-time*. Namun, pengawasan yang efektif memerlukan kolaborasi antara sektor publik dan swasta. Mishra et al. (2022) menekankan bahwa sinergi antara kedua sektor tersebut dapat meningkatkan efektivitas pengawasan melalui berbagi informasi dan sumber daya. Dengan pendekatan ini, risiko kebocoran data dapat diminimalkan, dan organisasi dapat meningkatkan kepercayaan publik terhadap sistem keamanan mereka.

Kepatuhan terhadap regulasi juga membutuhkan komitmen dari manajemen tingkat atas. Proses pelaporan insiden yang transparan dan tindakan korektif yang segera adalah langkah-langkah penting yang memastikan keberhasilan implementasi regulasi. Pelatihan rutin bagi karyawan di semua tingkat organisasi menjadi elemen penting lainnya untuk memastikan pemahaman yang mendalam tentang pentingnya pengawasan dan kepatuhan.

Kesadaran dan Edukasi

Kesadaran dan edukasi tentang keamanan siber merupakan elemen vital untuk mencegah pencurian data. Penelitian menemukan bahwa banyak kasus pencurian data disebabkan oleh kelalaian manusia, seperti penggunaan kata sandi yang lemah atau klik pada tautan phishing. Contoh kasus yang menarik perhatian adalah penggunaan kata sandi default "Admin#1234" untuk mengakses server Pusat Data Nasional Sementara (PDNS). Bahkan, kata sandi yang dinilai lemah tersebut juga bisa digunakan untuk mengakses server Badan Pengawasan Keuangan dan Pembangunan (BPKP) oleh siapapun (Andhika, 2024). Insiden tersebut menunjukkan betapa pentingnya edukasi yang tepat tentang praktik keamanan siber.

Chaudhary et al. (2022) menunjukkan bahwa program kesadaran siber yang dirancang dengan baik dapat mendorong individu dan organisasi untuk mengambil langkah-langkah protektif yang lebih baik. Pendekatan berbasis skenario, seperti simulasi serangan phishing, dapat membantu meningkatkan pemahaman tentang ancaman yang dihadapi. Selain itu, edukasi berkelanjutan memastikan bahwa karyawan tetap waspada terhadap ancaman baru yang terus berkembang.

Kasus pencurian data nasional pada tahun 2024 menunjukkan bahwa edukasi yang kurang menjadi salah satu faktor utama kerentanan. Penelitian merekomendasikan program pelatihan yang wajib bagi karyawan di semua tingkat organisasi. Program tersebut harus mencakup pemahaman dasar tentang keamanan informasi, praktik terbaik dalam penggunaan kata sandi, dan cara mendeteksi ancaman siber.

Edukasi yang efektif juga mencakup pengembangan modul pembelajaran yang mudah dipahami oleh semua lapisan karyawan. Pemanfaatan teknologi, seperti platform e-learning, dapat menjadi solusi untuk menjangkau lebih banyak peserta dengan biaya yang efisien. Pendekatan komprehensif ini tidak hanya meningkatkan kesadaran individu tetapi juga menciptakan budaya organisasi yang lebih sadar akan pentingnya keamanan siber.

Kolaborasi Antar Lembaga dan Sektor

Kolaborasi antar lembaga dan sektor menjadi strategi penting dalam menciptakan keamanan siber yang tangguh. Ancaman siber yang semakin kompleks membutuhkan pendekatan kolektif yang melibatkan berbagai pihak, termasuk pemerintah, sektor swasta, dan komunitas internasional. Penelitian menemukan bahwa sinergi tersebut memungkinkan berbagi informasi, sumber daya, dan teknologi yang lebih efektif.

Mishra et al. (2022) menunjukkan bahwa kolaborasi lintas sektor dapat mempercepat respons terhadap ancaman siber. Misalnya, berbagi intelijen tentang metode serangan terbaru dapat membantu organisasi lain untuk mempersiapkan diri. Selain itu, kerja sama internasional diperlukan untuk menghadapi ancaman lintas batas, seperti ransomware yang menyasar berbagai negara secara simultan.

Penelitian merekomendasikan pembentukan forum kolaborasi yang melibatkan berbagai pemangku kepentingan. Forum tersebut dapat berfungsi sebagai platform untuk berbagi praktik terbaik, mengembangkan standar keamanan global, dan mendiskusikan strategi untuk menghadapi ancaman baru. Dengan pendekatan ini, ekosistem digital yang lebih aman dan adaptif dapat tercipta, mendukung pertumbuhan ekonomi dan stabilitas nasional.

Kolaborasi juga dapat diwujudkan melalui kemitraan publik-swasta yang mendukung pengembangan teknologi baru. Pemerintah dapat memberikan insentif kepada perusahaan untuk berinvestasi dalam solusi keamanan canggih, sementara sektor swasta dapat berbagi inovasi dengan lembaga pemerintah untuk memperkuat perlindungan data. Strategi tersebut memastikan bahwa semua pihak memiliki peran aktif dalam menjaga keamanan siber yang berkelanjutan.

KESIMPULAN

Kesimpulan penelitian menegaskan bahwa regulasi komunikasi yang efektif merupakan elemen kunci dalam mengatasi ancaman pencurian data nasional. Temuan penelitian menunjukkan bahwa kebijakan keamanan siber yang komprehensif harus diterapkan secara konsisten untuk melindungi informasi sensitif. Sebagai contoh, penggunaan enkripsi yang kuat, autentikasi dua faktor, dan pengelolaan kata sandi yang kompleks menjadi langkah mendasar yang harus diwujudkan. Tanpa langkah-langkah tersebut, organisasi akan terus menghadapi risiko serangan siber, seperti kasus penggunaan kata sandi sederhana yang mengakibatkan kebocoran data masif. Temuan tersebut memberikan implikasi yang signifikan, baik secara praktis maupun akademis.

Dari sudut pandang praktis, hasil penelitian dapat digunakan oleh pembuat kebijakan untuk merancang regulasi yang lebih spesifik dan adaptif, terutama dalam mengantisipasi ancaman siber yang terus berkembang. Selain itu, organisasi dapat mengambil pelajaran dari temuan tersebut untuk meningkatkan pengawasan internal dan memperkuat pelatihan karyawan dalam menjaga keamanan data. Program kesadaran dan edukasi yang berkelanjutan menjadi rekomendasi penting, karena kesalahan manusia seringkali menjadi faktor utama dalam

pelanggaran keamanan. Temuan tersebut juga menggarisbawahi pentingnya kerja sama lintas sektor antara pemerintah, sektor swasta, dan komunitas internasional dalam memperkuat sistem keamanan kolektif.

Dari sudut pandang akademis, penelitian memberikan kontribusi terhadap pengembangan teori regulasi komunikasi dalam konteks keamanan siber. Penelitian memperluas pemahaman tentang bagaimana kebijakan dan regulasi dapat berperan sebagai alat mitigasi terhadap ancaman siber, sekaligus membuka peluang untuk penelitian lanjutan. Sebagai contoh, eksplorasi lebih lanjut tentang efektivitas teknologi keamanan tertentu atau dampak kolaborasi lintas sektor terhadap penurunan kasus pencurian data. Dengan demikian, temuan tersebut tidak hanya relevan untuk mengatasi tantangan praktis, tetapi juga memberikan dasar teoritis yang kuat bagi studi-studi di masa depan. Manfaat yang dihasilkan menjadi referensi penting dalam upaya meningkatkan ketahanan siber secara global.

DAFTAR PUSTAKA

Adhikari, S. (2024). Necessity of Big Data Security and its Relation to National Security. *Unity Journal*, *5*(1), 1–14. https://doi.org/10.3126/unityj.v5i1.63137

Adnani, K. (2021). *Metodologi Penelitian Komunikasi Kualitatif dan Kuantitatif* (Firts). Efudepress. https://eprints.iain-surakarta.ac.id/5064/1/14.

Andhika, I. K. (2024). *"ADMIN#1234" Ternyata Password Untuk Akses Server PDN*. 06 Juli. https://www.rri.co.id/iptek/806581/admin-1234-ternyata-password-untuk-akses-server-pdn

Bahtiar, N. (2022). Darurat Kebocoran Data : Kebutuhan Regulasi Pemerintah. *Development Policy and Management Review (DPMR)*, *2*(1), 1–16. file:///C:/Users/user/Downloads/32144-Article Text-109597-1-10-20240320.pdf

Chaudhary, S., Gkioulos, V., & Katsikas, S. (2022). Developing metrics to assess the effectiveness of cybersecurity awareness program. *Journal of Cybersecurity*, *8*(1), 1–19. https://doi.org/10.1093/cybsec/tyac006

Feintuck, M., & Varney, M. (2006). *Media Regulation, Public Interest, and the Law*. Edinburgh University Press Ltd.

Li, L., He, W., Xu, L., Ash, I., Mohd Anwar, & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, 13–14. https://doi.org/https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Mishra, A., Alzoubi, Y. I., Gill, A. Q., & Anwar, M. J. (2022). Cybersecurity Enterprises Policies: A Comparative Study. *Sensors*, *22*(2), 1–35. https://doi.org/10.3390/s22020538

Nugroho, I. H. D., Pebriawan, K., Jati, K. G. T. M., Diptha, I. G. C. A., Listartha, I. M. E., & Saskara, G. A. J. (2023). Analisa Evaluasi Kinerja Software Password Attacker Pada Berkas File Zip. *Jurnal Informatika Dan Tekonologi Komputer (JITEK)*, *3*(1), 14–23. https://doi.org/10.55606/jitek.v3i1.899

Rianto, P. (2019). Perbandingan Paradigma Otoritarianisme dan Demokrasi dalam Regulasi Media Massa di Indonesia. *JURNAL IPTEKKOM : Jurnal Ilmu Pengetahuan & Teknologi Informasi*, *21*(2), 123. https://doi.org/10.33164/iptekkom.21.2.2019.123-138

Rianto, P. (2024). *Regulasi komunikasi: tantangan di era media baru* (Firts). UII Press Yogyakarta.

Sarjito, A. (2024). Data Security and Privacy in the Digital Era : Challenges for Modern Government. *JIAN (Jurnal Ilmiah Administrasi Negara)*, *8*(3), 1–13. https://ojs.ejournalunigoro.com/index.php/JIAN