KARAKTERISTIK ANCAMAN SIBER PADA DIREKTORAT JENDERAL BINA ADMINISTRASI KEWILAYAHAN KEMENTERIAN DALAM NEGERI REPUBLIK INDONESIA

Wira Fattah Pasha
NPP. 32.0879
Asdaf Kota Palu, Provinsi Sulawesi Tengah
Program Studi Teknologi Rekayasa Informasi Pemerintahan
Email: wirafattah21@gmail.com

Pembimbing Skripsi: Sudarmono, S.STP, M.Si, Ph.D.

ABSTRACT

Problem Statement/Background (GAP): *This study focuses on the frequent occurrences of cyberattacks targeting the Ministry of Home Affairs of the Republic of Indonesia, as well as the absence of specific data on cyber incidents affecting individual government institutions in the country.* ***Purpose:*** *The objective of this research is to identify and classify the types of cyber threats targeting the Directorate General of Regional Administration at the Ministry of Home Affairs of the Republic of Indonesia, and to analyze the underlying motives behind these attacks.* ***Method:*** *This study employs a quantitative descriptive approach using the MITRE ATT&CK framework for classification. The data is sourced from reports provided from Pusdatin.* ***Result:*** *The findings reveal that the most frequent cyberattacks are Distributed Denial of Service (DoS) and Vulnerability Scanning. The motives behind these cyberattacks include disrupting governmental operations, exploiting system vulnerabilities, and stealing or manipulating sensitive data.* ***Conclusion:*** *The classification of incidents using the MITRE ATT&CK framework indicates that DoS attacks and vulnerability scanning are the primary attack vectors targeting the Directorate General of Regional Administration. Understanding the motives—ranging from service disruption to data exfiltration—serves as a critical foundation for designing more comprehensive cybersecurity strategies. It is recommended that the government enhance real-time monitoring, implement strict patch management, and improve cybersecurity awareness through training for all personnel to strengthen the resilience of digital public administration systems.*

Keywords: Cyber Threats, E-Government, Dos Attacks, Vulnerability Scanning, Information Security

ABSTRAK

Permasalahan/Latar Belakang (GAP): Penulis berfokus pada seringnya terjadi serangan siber pada Kementerian Dalam Negeri Republik Indonesia dan tidak adanya data serangan siber yang spesifik pada suatu instansi pemerintah di Indonesia. **Tujuan:** Tujuan dari penelitian ini adalah untuk mengidentifikasi dan mengklasifikasikan jenis-jenis ancaman siber yang menargetkan Direktorat Jenderal Bina Administrasi Kementerian Dalam Negeri Republik Indonesia dan menganalisis motif di balik serangan-serangan tersebut. **Metode:** Penelitian ini menggunakan metode kuantitatif deskriptif menggunakan klasifikasi MITRE ATT&CK yang mana datanya bersumber dari laporan Pusdatin. **Hasil/Temuan:** Temuan yang diperoleh penulis dalam penelitian ini yaitu serangan siber yang paling sering terjadi adalah Distributed Denial of Service (DoS) dan Vulnerability Scanning yang mana motif pelaku serangan siber adalah gangguan operasional pemerintahan, eksploitasi kerentanan sistem, dan pencurian atau manipulasi data sensitif. **Kesimpulan:** Klasifikasi insiden menggunakan kerangka MITRE ATT&CK menunjukkan bahwa DoS dan vulnerability scanning merupakan vektor serangan utama terhadap Direktorat Jenderal Bina Administrasi Kewilayahan. Pemahaman motif—mulai dari upaya mengganggu layanan hingga mengeksfiltrasi data—menjadi dasar penting untuk merancang strategi keamanan siber yang lebih menyeluruh. Disarankan agar pemerintah memperkuat monitoring real-time, menerapkan manajemen patch yang ketat, dan meningkatkan kesadaran siber melalui pelatihan bagi seluruh pegawai untuk memperkuat ketahanan sistem administrasi publik digital.

Kata kunci: Cyber Threats, E-Government, Dos Attacks, Vulnerability Scanning, Information Security

I. PENDAHULUAN

1.1. Latar Belakang

Penerapan TIK dalam penyelenggaraan pemerintahan—terutama melalui inisiatif e-government—telah mendorong percepatan proses administrasi, transparansi, dan partisipasi publik. Berbagai portal layanan online, sistem manajemen data terintegrasi, dan aplikasi mobile memudahkan warga dalam mengurus keperluan administratif, sekaligus menyediakan data secara terbuka dan real-time untuk memantau kinerja pemerintah. Meskipun masih dihadapkan pada tantangan infrastruktur, keterbatasan SDM terampil, dan resistensi birokrasi, investasi berkelanjutan pada pelatihan, teknologi, dan kebijakan pendukung telah menunjukkan hasil positif dalam meningkatkan efektivitas dan efisiensi pelayanan publik.

Sebagai unit yang bertanggung jawab atas administrasi kewilayahan, Ditjen Bina Administrasi Kewilayahan Kemendagri memerlukan dukungan TIK yang andal dan aman untuk menjalankan fungsi otonomi daerah hingga pemantauan pelaksanaan kebijakan. Kompleksitas tugas mengharuskan adopsi kerangka kerja keamanan siber komprehensif—meliputi tata kelola, penilaian risiko, kontrol teknis, respons insiden, serta kolaborasi dengan lembaga keamanan nasional dan internasional. Investasi pada model mitigasi seperti Ransomware Risk Management Model (R2M2) dan pelibatan ekosistem eksternal penting untuk menjaga integritas, kerahasiaan, dan ketersediaan layanan.

Di era ancaman siber yang kian canggih—termasuk phishing, ransomware, DDoS, dan APT—pendekatan sistematis seperti MITRE ATT&CK sangat diperlukan untuk mengidentifikasi taktik, teknik, dan prosedur penyerang. Analisis data BSSN pada Agustus 2024, yang mencatat lonjakan anomali hingga lebih dari satu juta kejadian per hari dan dominasi malware serta trojan, menegaskan urgensi pemantauan dini dan klasifikasi ancaman secara spesifik terhadap instansi pemerintah. Dengan pemahaman motivasi pelaku serangan dan pola serangan yang terstruktur, Ditjen Bina Administrasi

Kewilayahan dapat merumuskan strategi pertahanan yang proaktif dan menyesuaikan kebijakan keamanan siber sesuai kebutuhan lokal.

1.2. Kesenjangan Masalah yang Diambil (GAP Penelitian)

Pemerintahan telah memanfaatkan kemajuan teknologi informasi dan komunikasi (TIK) untuk mempermudah penyebaran informasi melalui media digital, sehingga hampir semua aspek kehidupan masyarakat kini terhubung secara online (Dimas et al., 2024; Tumija et al., 2024). Salah satu wujud implementasi TIK ini adalah e-government, yang menjadi strategi utama pemerintah dalam meningkatkan efisiensi administrasi, transparansi, dan partisipasi publik dalam pengambilan keputusan (Zulmasyhur et al., 2024:1). Namun, Wirtz dan Weyerer (2016:1) menegaskan bahwa operasional keamanan siber di sektor publik masih "kotak hitam" yang minim kajian, padahal kebutuhan dan karakteristik ancaman di tiap instansi—termasuk perangkat keras, perangkat lunak, dan pola lalu lintas data—dapat berbeda satu sama lain.

Dalam konteks Direktorat Jenderal Bina Administrasi Kewilayahan Kemendagri, penelitian khusus tentang ancaman siber masih sangat terbatas. Kompleksitas serangan terus meningkat dan menuntut alat pertahanan yang lebih canggih daripada sekadar firewall atau antivirus tradisional (Ahmed et al., 2024:5). Sebagian besar studi sebelumnya lebih berfokus pada kementerian pusat atau badan usaha negara, sehingga pola serangan dan konfigurasi sistem di Direktorat Jenderal ini belum tergambarkan dengan jelas. Padahal, menurut Geometripolitic, ancaman siber terbagi menjadi dua domain utama—high-politics (militer) dan low-politics (sipil)—yang memerlukan pendekatan keamanan berbeda (Arianto & Anggraini, 2019:3). Sementara itu, pelayanan publik di Indonesia terus menjadi sorotan utama dalam penyelenggaraan pemerintahan (Qomara & Lareken, 2024).

Meskipun Badan Siber dan Sandi Negara (BSSN) melaporkan lonjakan anomali trafik siber hingga lebih dari satu juta kejadian per hari pada Agustus 2024 (BSSN, 2024), dokumentasi jenis serangan—seperti phishing, ransomware, DDoS, atau APT—serta dampaknya terhadap layanan publik di Ditjen Bina Adwil masih minim. Kebanyakan laporan hanya mencatat jumlah anomali secara agregat tanpa membedakan kategori ancaman, mencerminkan kurangnya sistem pemantauan real-time terintegrasi dan prosedur eskalasi insiden yang formal. Akibatnya, respons insiden cenderung reaktif dan terfragmentasi, serta sulit melakukan analisis tren jangka panjang untuk merancang kapabilitas deteksi dan respons yang adaptif.

1.3. Penelitian Terdahulu

Berbagai penelitian terdahulu menunjukkan urgensi dan kompleksitas dalam menghadapi ancaman siber. Al-Hawamleh (2023) melalui penelitian berjudul *Predictions of Cybersecurity Experts on Future Cyber-Attacks and Related Cybersecurity Measures* menekankan pentingnya tindakan pencegahan, seperti pemahaman metode serangan, penggunaan perangkat lunak keamanan, serta otorisasi dua faktor dan protokol backend baru untuk melindungi data dari peretas. Sementara itu, Bolun (2022) dalam *A Differentiated Beneficiary Cybersecurity Approach* mengusulkan pendekatan keamanan siber yang terstruktur berdasarkan kategori penerima manfaat—baik individu maupun organisasi—guna meningkatkan efektivitas implementasi dan efisiensi biaya. Adapun Riggs et al. (2023) dalam studinya *Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure* mengidentifikasi lonjakan serangan siber terhadap infrastruktur kritis, termasuk ransomware dan DDoS, serta menekankan pentingnya strategi mitigasi yang tepat. Tidak hanya itu, Abbas et al. (2024) dalam *Evaluating Deep Learning Variants for Cyber-Attacks Detection and Multi-Class Classification in IoT Networks* menunjukkan bahwa model deep learning—terutama RNN—dapat mendeteksi berbagai jenis serangan IoT dengan akurasi hingga 96,56%, memperkuat peran kecerdasan buatan dalam deteksi dini dan klasifikasi ancaman . Selain itu, Arianto & Anggraini (2019)

dalam *Building Indonesia's National Cyber Defense and Security* menyoroti kendala pengembangan keamanan siber di tingkat nasional—mulai dari rendahnya pemahaman pemerintah dan kelemahan industri lokal dalam memproduksi perangkat keras TI, hingga fragmentasi penanganan insiden dan kurangnya koordinasi antar-institusi—serta menegaskan perlunya kebijakan komprehensif dan standar infrastruktur pertahanan siber untuk melindungi infrastruktur vital seperti radar bandara Soekarno-Hatta . Kelima penelitian ini sama-sama menyoroti perlunya pendekatan yang adaptif dan menyeluruh dalam menghadapi ancaman keamanan digital yang terus berkembang.

1.4. Pernyataan Kebaruan Ilmiah

Penelitian ini merupakan studi pertama yang secara khusus mengidentifikasi dan mengklasifikasikan karakteristik ancaman siber di lingkungan Ditjen Bina Administrasi Kewilayahan Kemendagri menggunakan pendekatan kuantitatif deskriptif berbasis MITRE ATT&CK. Berbagai penelitian terdahulu—Al-Hawamleh (2023) tentang pencegahan serangan melalui otentikasi ganda dan protokol backend, Bolun (2022) dengan pendekatan berbasis kategori penerima manfaat, Riggs et al. (2023) yang menyoroti lonjakan ransomware dan DDoS pada infrastruktur kritis, Abbas et al. (2024) yang menghadirkan akurasi deteksi IoT hingga 96,56% menggunakan RNN, serta Arianto & Anggraini (2019) mengenai kelemahan koordinasi dan kebijakan nasional—semua menekankan perlunya strategi keamanan adaptif dan menyeluruh. Namun, dengan memanfaatkan data insiden nyata dari tim konsultan Pusdatin, penelitian ini mengungkap frekuensi serangan (misalnya DDoS, vulnerability scanning) dan motif pelaku layanan publik digital, sehingga mengisi kekosongan studi pada level instansi pemerintahan dan memberikan landasan empiris bagi kebijakan pertahanan siber yang kontekstual.

1.5. Tujuan.

Tujuan dari penelitian ini adalah untuk mengidentifikasi dan mengklasifikasikan jenis-jenis ancaman siber yang menargetkan Direktorat Jenderal Bina Administrasi Kementerian Dalam Negeri Republik Indonesia dan menganalisis motif di balik serangan-serangan tersebut.

II. METODE

Penelitian ini menggunakan pendekatan kuantitatif deskriptif yang bertujuan untuk menggambarkan karakteristik ancaman siber yang terjadi di lingkungan Direktorat Jenderal Bina Administrasi Kewilayahan Kementerian Dalam Negeri Republik Indonesia. Pendekatan ini dipilih untuk memberikan pemahaman berbasis data terhadap jenis, pola, dan tujuan serangan siber yang dialami oleh instansi tersebut. Penelitian ini tidak bertujuan menguji hipotesis, melainkan memetakan ancaman secara sistematis berdasarkan data insiden yang telah dikumpulkan.

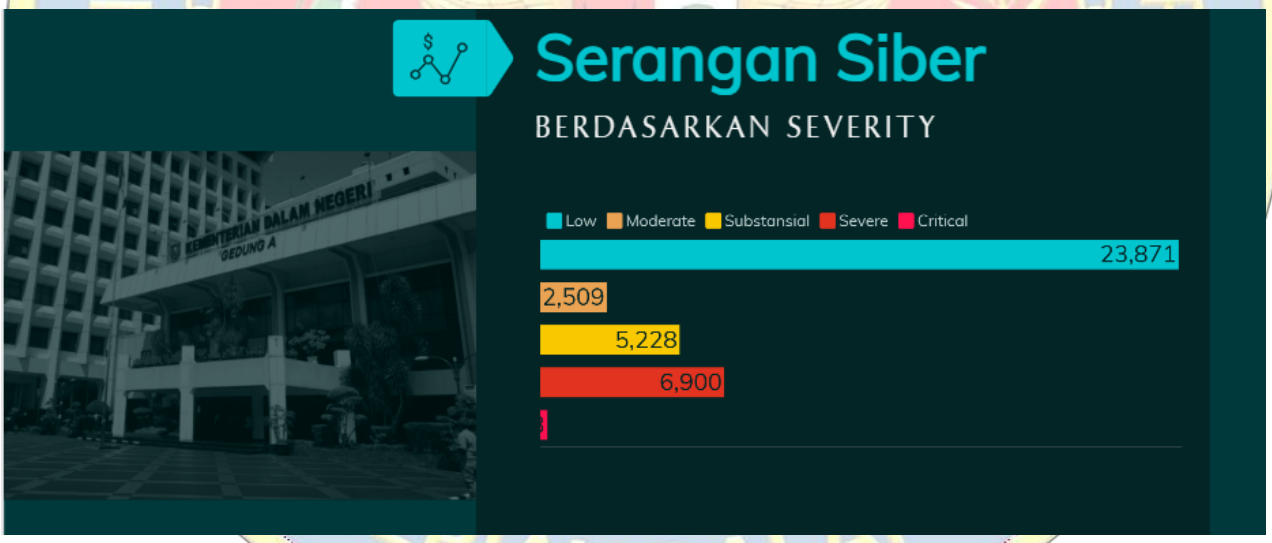
Penelitian ini menggunakan kerangka kerja *MITRE ATT&CK* sebagai alat bantu klasifikasi dan analisis ancaman siber. Melalui kerangka ini, setiap insiden dikategorikan berdasarkan taktik, teknik, dan prosedur (TTP) yang digunakan oleh pelaku serangan. Data kuantitatif yang diperoleh kemudian diolah dan disajikan dalam bentuk tabel dan grafik untuk mendeskripsikan kecenderungan jenis serangan yang dominan, arah serangan, serta potensi dampaknya terhadap sistem informasi. Teknik analisis yang digunakan adalah analisis statistik deskriptif untuk menggambarkan distribusi frekuensi dari masing-masing jenis ancaman yang teridentifikasi.

III. HASIL DAN PEMBAHASAN

Penulis menggunakan kerangka kerja MITRE ATT&CK untuk memetakan karakteristik ancaman siber di Direktorat Jenderal Bina Administrasi Kewilayahan Kementerian Dalam Negeri Republik Indonesia, dengan mengelompokkan insiden berdasarkan taktik, teknik, dan prosedur (TTP) pelaku serangan—data yang diperoleh dari tim konsultan Pusdatin kemudian dianalisis untuk mengidentifikasi jenis serangan dominan, arah serangan, dan motif di baliknya. Keamanan siber dalam konteks ini mencakup komponen-komponen kunci seperti tata kelola, kepemimpinan, penilaian, manajemen risiko, kontrol teknis, pelatihan, respons insiden, serta kolaborasi dengan pemangku kepentingan eksternal (Kumar et al., 2024:3). Tujuannya adalah mengurangi risiko yang mengancam organisasi dan penggunanya, termasuk melindungi aset–aset Internet of Things (IoT) dan menjaga privasi data (Lee, 2020:22). Namun, seiring dengan meningkatnya kompleksitas serangan, fokus perlindungan telah bergeser ke infrastruktur kritis nasional yang rentan terhadap ancaman canggih (Kim et al., 2021:3). Secara umum, keamanan siber mencakup praktik, alat, dan konsep pertahanan informasi serta teknologi operasional—tindakan defensif yang bergantung pada sistem dan lingkungan TI maupun OT untuk memitigasi potensi ancaman (Galinec et al., 2017:5). Hasil pemetaan dan pembahasan rinci akan disajikan pada subbab berikut.

3.1. Serangan berdasarkan Severity

Penulis memetakan karakteristik ancaman siber berdasarkan yang terjadi di Kementerian Dalam Negeri Republik Indonesia. emetaan ini dilakukan terhadap data insiden yang diperoleh dari tim konsultan Pusdatin guna mengidentifikasi jenis serangan yang dominan, arah serangan, serta motif yang melatarbelakanginya



Serangan siber yang terjadi di Direktorat Jenderal Bina Administrasi Kewilayahan menunjukkan variasi jenis serangan dengan pola yang acak atau tidak terprediksi. Namun, dari hasil pemetaan berdasarkan tingkat severity, diketahui bahwa mayoritas serangan berada pada level *low*. Hal ini menunjukkan bahwa meskipun serangan terjadi dengan frekuensi yang tinggi, tingkat keparahannya cenderung rendah. Serangan pada level ini umumnya tidak menyebabkan kerusakan serius secara langsung, tetapi tetap perlu diwaspadai karena dapat membuka celah terhadap serangan lanjutan yang lebih berbahaya.

3.2. Serangan berdasarkan Severity

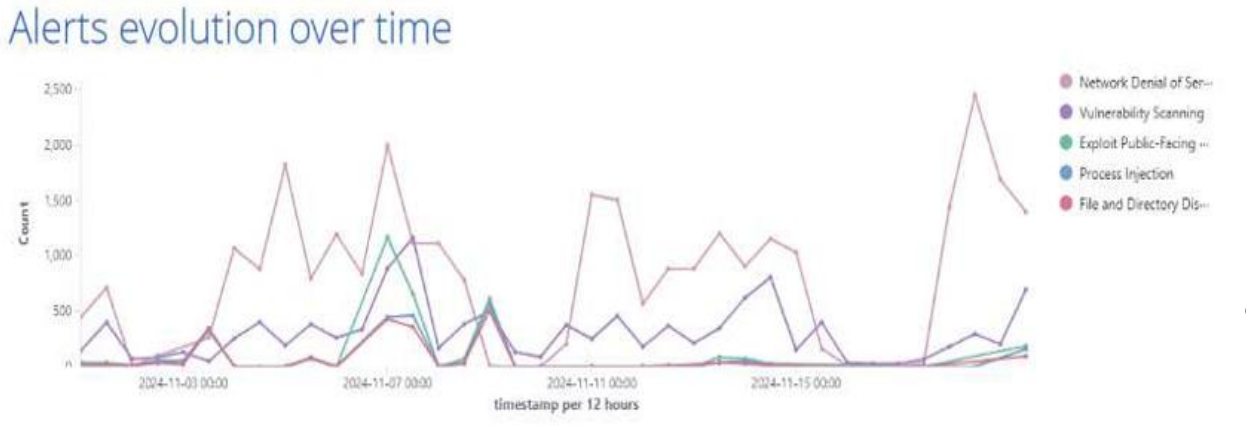
No	Rule ID	Description
1	550	Integrity Checksum Changed
2	554	File added to the system
3	553	File Deleted

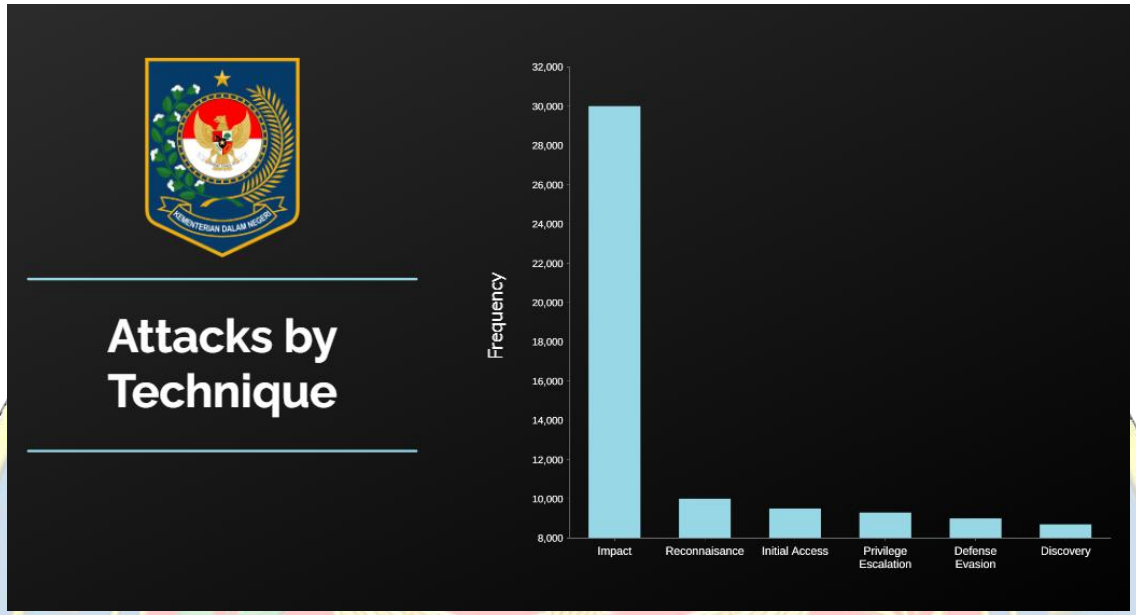
Dalam FIM (File Integrity Monitoring), alert yang paling sering muncul adalah "Integrity Checksum Changed" dan "*File added to the system*". Alert "*Integrity Checksum Changed*" menunjukkan adanya perubahan nilai checksum pada suatu file, yang mengindikasikan potensi modifikasi tidak sah dan ancaman terhadap sistem. Sementara itu, alert "*File added to the system*" menandakan penambahan file mencurigakan yang dapat dimanfaatkan oleh pelaku untuk keuntungan pribadi dan merugikan instansi.

Network Denial of Service (DoS) adalah serangan yang membanjiri sistem dengan permintaan hingga layanan tidak dapat digunakan. Jika dilakukan secara serentak dari banyak komputer, disebut *Distributed Denial of Service* (DDoS). Serangan ini sangat mengganggu layanan digital pemerintah. Sementara itu, *Vulnerability Scanning* adalah upaya mencari celah keamanan sistem dengan alat otomatis, sebagai langkah awal untuk serangan yang lebih berbahaya.

Salah satu target utama serangan siber adalah web SIPD, platform pemerintah untuk perencanaan, penganggaran, dan pelaporan keuangan. SIPD sering mengalami serangan *DoS* dan *Vulnerability Scanning.* Jika dibiarkan, ancaman ini dapat berdampak besar secara finansial dan reputasi negara. Terlebih lagi, dengan adanya FIM (*File Integrity Monitoring*), diketahui bahwa ancaman terhadap SIPD semakin meningkat.

Kelemahan konfigurasi atau sistem yang belum dipatch bisa dimanfaatkan peretas untuk mencuri atau memanipulasi data. Motif serangan bervariasi, mulai dari hacktivism, pencurian data sensitif, pemerasan dengan ransomware, hingga upaya melemahkan sistem pemerintahan. Ancaman siber menjadi salah satu tantangan utama yang dihadapi oleh instansi pemerintah di era digital saat ini. Organisasi dan individu menghadapi ancaman siber yang terus-menerus dari pelaku ancaman siber yang berusaha mengkompromikan keamanan jaringan dan mencuri informasi penting (Janoti et al., 2024:5).




Attacks by Technique
Frequency
32,000
30,000
28,000
26,000
24,000
22,000
20,000
18,000
16,000
14,000
12,000
10,000
8,000
Impact
Reconnaisance
Initial Access
Privilege Escalation
Defense Evasion
Discovery


TOP TACTICS
Impact
Reconnaissance
Equipment and supplies
Initial Access
Privilege Escalation
Defense Evasion
Discovery
Execution
Persistence
Lateral Movement
Credential Access

Pelaku serangan siber kerap melakukan kerusakan yang tampak frontal pada *user interface*, namun hal ini seringkali hanya pengalih perhatian dari serangan yang lebih serius. hacker merusak tampilan UI—kerusakan yang terkesan ringan dan mudah diperbaiki. Namun tak lama kemudian, server tidak dapat diakses, meskipun tidak ada tanda serangan lanjutan yang terdeteksi. Semua *password* server telah dicoba tetapi tak satupun berhasil, hingga akhirnya server dipaksa dibuka dengan risiko kehilangan data. Untungnya, pusdatin dan lembaga di bawah Kemendagri rutin melakukan pencadangan, sehingga dampak data bisa diminimalkan. Faktanya, setelah merusak UI, hacker telah masuk ke server dan mengganti password sehingga mengunci akses administrator. Ini membuktikan bahwa serangan yang tampak ringan bisa menyembunyikan eksploitasi serius. Kasus ini menegaskan pentingnya evaluasi mendalam terhadap setiap serangan, tak peduli seberapa ringan gejalanya. Selain itu, dibutuhkan aturan dan protokol yang optimal untuk penanganan dan pemeriksaan sistem pasca-serangan agar potensi kerusakan dapat dicegah sedini mungkin.

No.	Aplikasi	Domain	IP Public
1	WEB ADWIL	ditjenbinaadwil.kemendagri.go.id	38.210.85.163

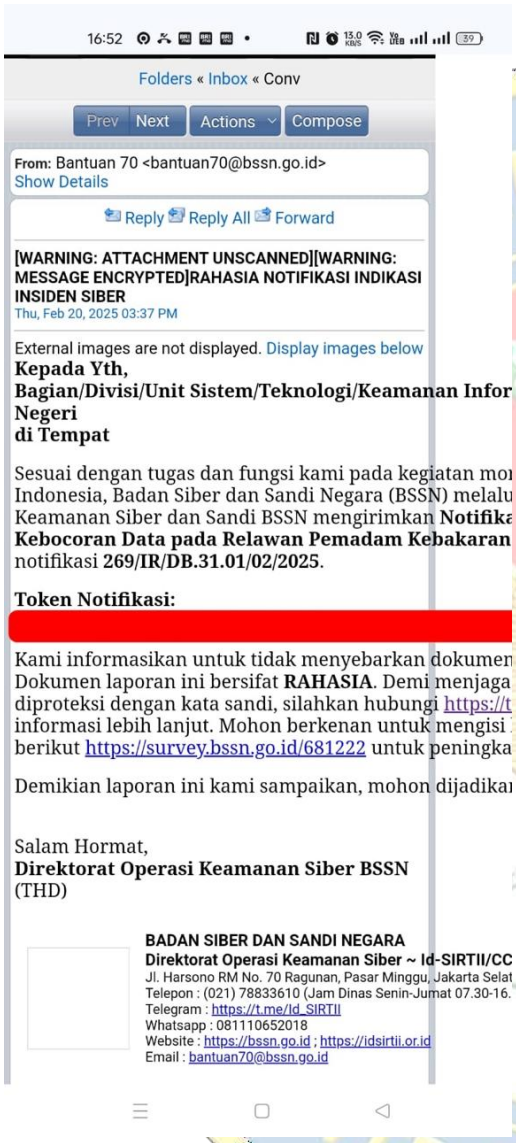
No.	Aplikasi	Domain	IP Public
2	CLOUD KEU	cloud-adwil.kemendagri.go.id	38.210.85.164
3	PAYROLL	payroll-adwil.kemendagri.go.id	38.210.85.165
4	EMONEV ADWIL	emonevadwil.kemendagri.go.id	38.210.85.166
5	KODE WILAYAH	kodewilayah.kemendagri.go.id	38.210.85.167
6	SIMSATPOL_PP	satpolpp.kemendagri.go.id	38.210.85.168
7	PERTANAHAN	pertanahan.kemendagri.go.id	38.210.85.169
8	SIMPEG_CUTI	simpeg-adwil.kemendagri.go.id	38.210.85.170
9	SIPGWPP	sipgwpp.kemendagri.go.id	38.210.85.171
10	PUU_ADWIL	puu-adwil.kemendagri.go.id	38.210.85.172
11	PAGAR SPM BENCANA	pagarspmbencana.kemendagri.go.id	38.210.85.173
12	DAMKAR	sidamkar.kemendagri.go.id	38.210.85.174
14	INDEKS BENCANA	indeks-suburusanbencana.kemendagri.go.id	38.210.85.175
15	DPMPTSP_EMONEV	emonev-dpmptsp.kemendagri.go.id	38.210.85.176
16	SIMPEL_SIAPKK	siapkk.kemendagri.go.id	38.210.85.177
17	TRANTIBUMLIMAS	trantibumlinmas.kemendagri.go.id	38.210.85.178
18	SIMLINMAS	simlinmas.kemendagri.go.id	38.210.85.179
19	SIRATU	siratu.kemendagri.go.id	38.210.85.180

No.	Aplikasi	Domain	IP Public
20	SDM_POLPP		38.210.85.181
21	KENCANA		38.210.85.182
25	LEGASI		38.210.85.186
26	ANGKET		38.210.85.187
28	SIPADAM		38.210.85.189
29	SIPADAM_REDKAR		38.210.85.190

Aplikasi-aplikasi yang digunakan oleh Ditjen Adwil telah mendukung berbagai kegiatan mereka secara digital, memberikan manfaat dalam efisiensi dan kecepatan proses. Namun, ketergantungan pada teknologi ini juga membuka peluang terhadap serangan siber.

Setiap aplikasi menyimpan data vital, termasuk dari unit seperti Damkar dan Polisi Pamong Praja. Meski sekilas data tersebut tampak kurang penting, justru bisa menjadi pintu masuk bagi peretas. Misalnya, data pegawai Damkar bisa digunakan untuk menyerang aplikasi lain yang lebih sensitif seperti Cloud KEU atau Payroll, karena kemungkinan penggunaan data login yang serupa.

Deteksi serangan siber dapat dilakukan melalui berbagai metode. Salah satunya adalah notifikasi dari BSSN (Badan Siber dan Sandi Negara) kepada Pusdatin, yang dikirimkan melalui aplikasi khusus. Notifikasi ini kemudian diikuti oleh surat resmi sebagai tindak lanjut dan bukti formal adanya potensi ancaman.



Folders « Inbox « Conv

Prev Next Actions Compose

From: Bantuan 70 <bantuan70@bssn.go.id>
Show Details

Reply Reply All Forward

[WARNING: ATTACHMENT UNSCANNED][WARNING: MESSAGE ENCRYPTED]RAHASIA NOTIFIKASI INDIKASI INSIDEN SIBER
Thu, Feb 20, 2025 03:37 PM

External images are not displayed. Display images below

Kepada Yth,
Bagian/Divisi/Unit Sistem/Teknologi/Keamanan Infor
Negeri
di Tempat

Sesuai dengan tugas dan fungsi kami pada kegiatan mo
Indonesia, Badan Siber dan Sandi Negara (BSSN) melalu
Keamanan Siber dan Sandi BSSN mengirimkan **Notifika**
Kebocoran Data pada Relawan Pemadam Kebakaran
notifikasi **269/IR/DB.31.01/02/2025**.

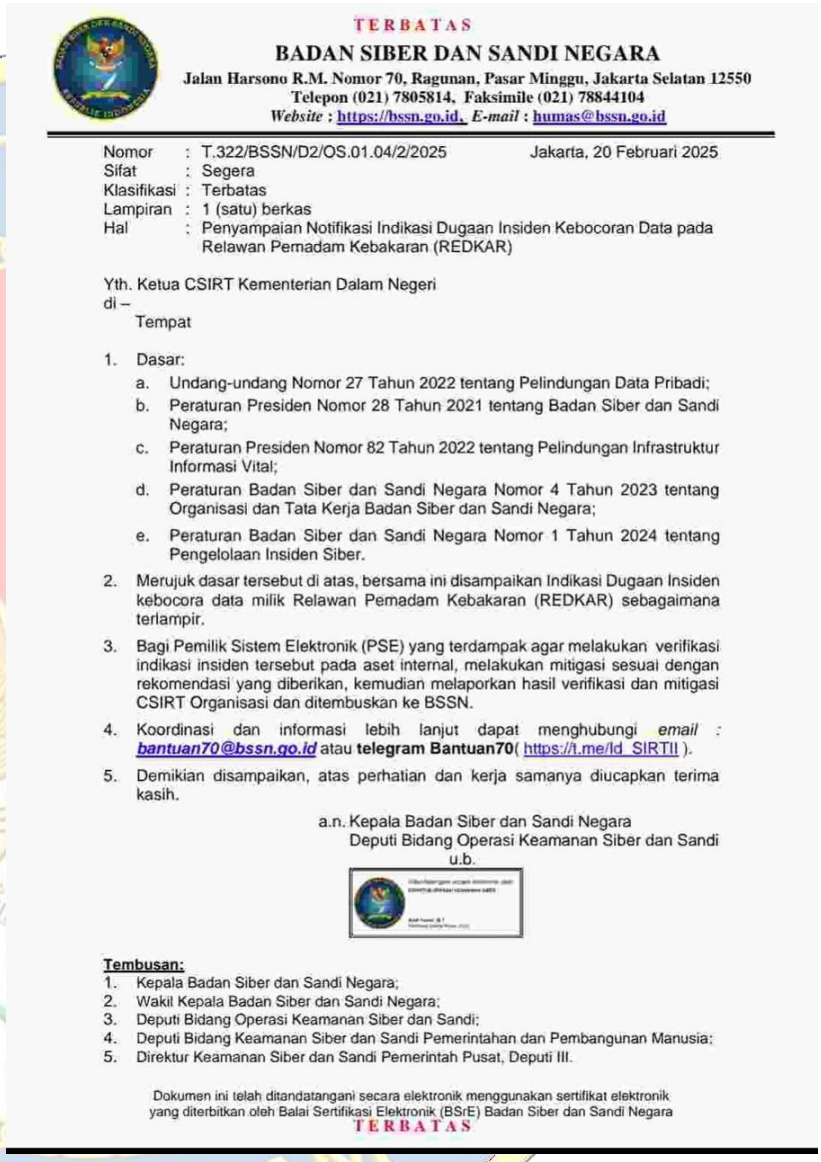
Token Notifikasi:

Kami informasikan untuk tidak menyebarkan dokumen
Dokumen laporan ini bersifat **RAHASIA**. Demi menjaga
diproteksi dengan kata sandi, silahkan hubungi https://t
informasi lebih lanjut. Mohon berkenan untuk mengisi
berikut https://survey.bssn.go.id/681222 untuk peningka

Demikian laporan ini kami sampaikan, mohon dijadika

Salam Hormat,
Direktorat Operasi Keamanan Siber BSSN
(THD)

BADAN SIBER DAN SANDI NEGARA
Direktorat Operasi Keamanan Siber ~ Id-SIRTII/CC
Jl. Harsono RM No. 70 Ragunan, Pasar Minggu, Jakarta Selat
Telepon : (021) 78833610 (Jam Dinas Senin-Jumat 07.30-16.
Telegram : https://t.me/Id_SIRTII
Whatsapp : 081110652018
Website : https://bssn.go.id ; https://idsirtii.or.id
Email : bantuan70@bssn.go.id



TERBATAS

BADAN SIBER DAN SANDI NEGARA
Jalan Harsono R.M. Nomor 70, Ragunan, Pasar Minggu, Jakarta Selatan 12550
Telepon (021) 7805814, Faksimile (021) 78844104
***Website* : https://bssn.go.id, *E-mail* : humas@bssn.go.id**

Nomor : T.322/BSSN/D2/OS.01.04/2/2025 Jakarta, 20 Februari 2025
Sifat : Segera
Klasifikasi : Terbatas
Lampiran : 1 (satu) berkas
Hal : Penyampaian Notifikasi Indikasi Dugaan Insiden Kebocoran Data pada Relawan Pemadam Kebakaran (REDKAR)

Yth. Ketua CSIRT Kementerian Dalam Negeri
di –
Tempat

1. Dasar:
   a. Undang-undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi;
   b. Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara;
   c. Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital;
   d. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2023 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara;
   e. Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber.
2. Merujuk dasar tersebut di atas, bersama ini disampaikan Indikasi Dugaan Insiden kebocora data milik Relawan Pemadam Kebakaran (REDKAR) sebagaimana terlampir.
3. Bagi Pemilik Sistem Elektronik (PSE) yang terdampak agar melakukan verifikasi indikasi insiden tersebut pada aset internal, melakukan mitigasi sesuai dengan rekomendasi yang diberikan, kemudian melaporkan hasil verifikasi dan mitigasi CSIRT Organisasi dan ditembuskan ke BSSN.
4. Koordinasi dan informasi lebih lanjut dapat menghubungi *email* : ***bantuan70@bssn.go.id*** atau **telegram Bantuan70**(https://t.me/Id_SIRTII).
5. Demikian disampaikan, atas perhatian dan kerja samanya diucapkan terima kasih.

a.n. Kepala Badan Siber dan Sandi Negara
Deputi Bidang Operasi Keamanan Siber dan Sandi
u.b.

Tembusan:
1. Kepala Badan Siber dan Sandi Negara;
2. Wakil Kepala Badan Siber dan Sandi Negara;
3. Deputi Bidang Operasi Keamanan Siber dan Sandi;
4. Deputi Bidang Keamanan Siber dan Sandi Pemerintahan dan Pembangunan Manusia;
5. Direktur Keamanan Siber dan Sandi Pemerintah Pusat, Deputi III.

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE) Badan Siber dan Sandi Negara

TERBATAS

3.2. Tujuan Pelaku Serangan Siber

Tujuan utama serangan siber umumnya berfokus pada pencurian/manipulasi data serta penghentian aktivitas pemerintahan. Data merupakan sasaran berharga karena dapat digunakan untuk mengeksploitasi sistem lebih lanjut. Salah satu bentuk umum serangan ini adalah *Distributed Denial of Service* (DDoS) yang melumpuhkan layanan publik dan dapat dianggap sebagai bentuk ancaman terhadap stabilitas nasional.

Pelaku biasanya menargetkan data pegawai, akun admin, dan informasi sensitif lainnya. Jika akun admin berhasil diretas, pelaku bisa menciptakan akun baru, mengunci akses admin asli, dan membocorkan data penting. Ini dapat menyebabkan kerusakan besar pada sistem, terutama pada sistem krusial seperti web SIPD. Gangguan pada SIPD dapat menghambat perencanaan, penganggaran, dan pelaporan keuangan, serta menunda distribusi anggaran untuk layanan publik dan pembangunan.

Beberapa serangan juga dilakukan sebagai distraksi. Misalnya, pelaku merusak tampilan sistem lebih dulu agar pengelola fokus memperbaikinya, padahal serangan utamanya adalah pembobolan otoritas sistem. Bila tidak ditelusuri secara menyeluruh, pelaku bisa mengakses sistem secara penuh tanpa terdeteksi. Dalam salah satu kasus, anomali server berhasil dideteksi dan sistem segera dihapus karena memiliki backup.

Kasus ini menegaskan pentingnya pencadangan dan pemeriksaan sistem menyeluruh sebagai prosedur tetap. Pemerintah perlu membuat peraturan yang memuat spesifikasi teknis pencadangan dan pemeriksaan sistem, khususnya karena daerah mungkin belum memiliki kesiapan seperti kementerian pusat. Hal ini penting demi meningkatkan kualitas dan ketahanan keamanan data pemerintahan.

3.3. Diskusi Temuan Utama Penelitian

Sama halnya dengan temuan AL-Hawamleh (AL-Hawamleh, 2023) bahwa Distributed Denial of Service (DDoS) termasuk serangan paling sering terjadi, penulis juga mencatat DDoS bersama Vulnerability Scanning sebagai vektor utama pada instansi Ditjen Bina Adwil Kemendagri . Berbeda dengan AL-Hawamleh yang menempatkan Password Spraying dan Ransomware sebagai ancaman dominan, penulis justru mengidentifikasi Vulnerability Scanning sebagai serangan paling frekuen . Sama halnya dengan motif data breach dan financial gain yang diungkap AL-Hawamleh, penulis menegaskan bahwa eksploitasi kerentanan dan manipulasi data sensitif menjadi motif sentral di lingkungan pemerintahan daerah . Temuan ini memperkuat rekomendasi proaktif untuk two-factor authentication, AI-driven protocols, dan back-end security enhancements yang diajukan AL-Hawamleh dengan anjuran real-time monitoring, manajemen patch ketat, dan pelatihan kesadaran siber dari penulis. Berbeda dengan proyeksi AL-Hawamleh yang menekankan peran AI dan cloud-based IAM pasca-COVID-19, penulis lebih menggarisbawahi penguatan prosedur operasional dan backup rutin sesuai karakteristik objek penelitian yang lebih lokal.

Temuan Bolun (Bolun, 2022) bahwa jenis serangan seperti Malware, Phishing, DDoS, dan SQL Injection merupakan ancaman umum yang sering terjadi pada berbagai sektor kritis, penulis juga mencatat bahwa serangan DDoS termasuk yang paling dominan terjadi pada Direktorat Jenderal Bina Administrasi Kewilayahan Kemendagri. Berbeda dengan penelitian Bolun (2022) yang fokus pada tipologi dan pengkategorian tingkat kebutuhan keamanan siber berdasarkan jumlah karyawan dan sektor industri, penelitian penulis lebih menitikberatkan pada deteksi jenis serangan aktual dan analisis terhadap celah sistem yang dimanfaatkan pelaku, khususnya melalui vulnerability scanning. Temuan ini memperkuat argumen bahwa pendekatan keamanan siber harus disesuaikan dengan karakteristik institusi, karena penulis menunjukkan bahwa institusi pemerintahan daerah memiliki kerentanan spesifik yang memerlukan strategi mitigasi yang berbeda dari pendekatan berbasis klasifikasi ukuran organisasi yang diajukan oleh Bolun (2022). Di sisi lain, temuan penulis menolak pendekatan generik yang tidak mempertimbangkan karakteristik lingkungan pemerintahan lokal yang terbatas dalam sumber daya teknis dan personel, sementara Bolun (2022) menekankan pentingnya diferensiasi tetapi belum menjabarkan secara mendalam implementasi di sektor publik pemerintahan daerah. Maka, keduanya sepakat bahwa pendekatan diferensial diperlukan, namun fokus objek dan konteks pelaksanaannya berbeda sesuai latar institusional masing-masing.

Sama halnya dengan temuan Riggs et al. (2023) yang mengidentifikasi berbagai jenis serangan utama—mulai dari DDoS, ransomware, phishing, hingga false data injection—yang mengancam keberlangsungan critical infrastructure secara global serta memproyeksikan lebih dari 1.100 insiden signifikan dalam lima tahun ke depan , penulis juga menemukan bahwa DDoS dan vulnerability scanning menempati posisi teratas sebagai vektor serangan pada Direktorat Jenderal Bina Administrasi Kewilayahan Kemendagri . Berbeda dengan Riggs et al. yang menyajikan kerangka mitigasi dan standar internasional (ISO, NIST, MITRE) untuk CI secara menyeluruh , penulis lebih

menitikberatkan pada tindakan operasional—seperti manajemen patch ketat, real-time monitoring, dan pelatihan kesadaran siber—sesuai karakteristik dan keterbatasan sumber daya instansi pemerintahan daerah . Temuan ini memperkuat pentingnya pendekatan berlapis (defense-in-depth) dan diferensiasi strategi keamanan, karena meski kedua penelitian sepakat bahwa CI membutuhkan tindakan proaktif dan beragam lapisan pertahanan, konteks penerapannya—global vs. lokal—membutuhkan adaptasi kebijakan dan teknologi yang berbeda.

IV. KESIMPULAN

Direktorat Jenderal Bina Administrasi Kewilayahan Kementerian Dalam Negeri RI, yang bertugas mengelola administrasi dan pembangunan daerah, kini semakin bergantung pada sistem digital sehingga rentan terhadap serangan Network Denial of Service dan Vulnerability Scanning. Meskipun penggunaan aplikasi digital meningkatkan efisiensi kerja, hal ini juga membuka celah bagi peretas untuk mencuri atau merusak data penting. Oleh karena itu, perlu diperkuat regulasi keamanan siber dan kapasitas pegawai dalam mendeteksi serta merespons ancaman, sembari menjalankan pencadangan data secara rutin dan melakukan audit keamanan (audit dan penetration testing) secara berkala. Dengan langkah-langkah tersebut, data akan tetap terlindungi, layanan publik terjamin kelancarannya, dan sistem pemerintahan semakin tahan terhadap serangan siber.

Keterbatasan Penelitian. Penelitian ini memiliki keterbatasan utama yakni waktu dan biaya penelitian.

Arah Masa Depan Penelitian (*future work*). Penulis menyadari masih awalnya temuan penelitian, oleh karena itu penulis menyarankan agar dapat dilakukan penelitian lanjutan pada lokasi serupa berkaitan dengan ancaman siber untuk menemukan hasil yang lebih mendalam.

V. UCAPAN TERIMA KASIH

Ucapan terima kasih terutama ditujukan kepada Ditjen Adwil dan Pusdatin Kemendagri yang telah memberikan kesempatan penulis untuk melaksanakan penelitian, serta seluruh pihak yang membantu dan mensukseskan pelaksanaan penelitian.

VI. DAFTAR PUSTAKA

Abbas, S., Ojo, S., Al Hejaili, A., Gregus, M., Bouazzi, I., Sampedro, G. A., & Almadhor, A. (2024). Evaluating deep learning variants for cyber-attacks detection and multi-class classification in IoT networks. *PeerJ. Computer Science, 10*, e1793. https://doi.org/10.7717/peerj-cs.1793

Ahmed, D. S., Abdulhameed, A. A., & Gaata, M. T. (2024). A systematic literature review on cyber attack detection in software-defined networking (SDN). *Mesopotamian Journal of CyberSecurity, 4*(3), 86–135. https://doi.org/10.58496/mjcs/2024/018

Arianto, A. R., & Anggraini, G. (2019). Building Indonesia's National Cyber Defense and Security to Face the Global Cyber Threats Through Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII). *Jurnal Pertahanan & Bela Negara, 9*(1), 17. https://doi.org/10.33172/jpbh.v9i1.515

Al-Hawamleh, A. M. (2023). Predictions of cybersecurity experts on future cyber-attacks and related cybersecurity measures. *International Journal of Advanced Computer Science and Applications, 14*(2), 801–809.

Badan Siber dan Sandi Negara. (2023). *Lanskap Keamanan Siber Indonesia 2023*. Badan Siber dan Sandi Negara.

Bolun, I., & Cojocaru, S. (2022, October). A differentiated beneficiary cybersecurity approach. In *Proceedings of the 12th International Conference on Electronics, Communications and Computing (IC ECCO-2022)* (pp. 115–118). Chisinau, Republic of Moldova. https://doi.org/10.52326/ic-ecco.2022/SEC.01

Dimas, M., & Fahlevvi, M. R. (2024). Pengentasan digital divide dalam penerapan e-Government di Kabupaten Sumbawa. *Jurnal Teknologi dan Komunikasi Pemerintahan, 6*(2), 194–215. https://doi.org/10.33701/jtkp.v6i2.4504

Galinec, D., Možnik, D., & Guberina, B. (2017). Cybersecurity and cyber defence: National level strategic approach. *Automatika, 58*(3), 273–286. https://doi.org/10.1080/00051144.2017.1407022

Janoti, N. S., Negi, N., Rohan, R., & Rida, R. (2024). Strategic perspectives on cyber threat intelligence: A comprehensive analysis. *International Journal for Research in Applied Science and Engineering Technology, 12*(4), 524–529. https://doi.org/10.22214/ijraset.2024.59816

Kim, K., Alfouzan, F. A., & Kim, H. (2021). Cyber-attack scoring model based on the offensive cybersecurity framework. *Applied Sciences, 11*(16), 7738. https://doi.org/10.3390/app11167738

Kumar, A., Kumar Mahto, R., Kumar Mishra, B., & Mishra, K. (2024). A framework for institution to enhancing cybersecurity in higher education: A review. *LatIA, 2*, 94. https://doi.org/10.62486/latia202494

Lee, I. (2020). Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. *Future Internet, 12*(9), 157. https://doi.org/10.3390/fi12090157

Qomara, E., & Lareken, M. E. (2024). Analisis perbaikan pelayanan pengaduan masyarakat Belitung Saluran Aspirasi dan Pengaduan (BESADU) di Kabupaten Belitung (Studi pada Dinas Komunikasi dan Informatika). *Jurnal Teknologi dan Komunikasi Pemerintahan, 6*(2), 259–285. https://doi.org/10.33701/jtkp.v6i2.4663

Riggs, A., He, Z., & Zhu, Q. (2023). Cybersecurity risk assessment and mitigation for critical infrastructures: Survey, trends, and open issues. *Sensors, 23*(10), 4060. https://doi.org/10.3390/s23104060

Tumija, & Kafi, F. (2024). Optimalisasi penggunaan website Newsroom dalam meningkatkan pelayanan informasi berbasis elektronik. *Jurnal Teknologi dan Komunikasi Pemerintahan, 6*(2), 238–258. https://doi.org/10.33701/jtkp.v6i2.4636

Wirtz, B. W., & Weyerer, J. C. (2016). Cyberterrorism and cyber attacks in the public sector: How public administration copes with digital threats. *International Journal of Public Administration, 40*(13), 1085–1100. https://doi.org/10.1080/01900692.2016.1242614

Zulmasyhur, Z., L. W., N. P., & Setiawan, H. D. (2024). Enhancing governance through digital transformation. *Jurnal Governansi, 10*(1), 127–136. https://doi.org/10.30997/jgs.v10i1.11544